K. Bulota, P. Survila

Algebra ir skaičių teorija

2

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \dots}}$$

K.Bulota, P.Survila

Algebra ir skaičių teorija

2

Antrasis pataisytas ir papildytas leidimas

Lietuvos švietimo ir kultūros ministerijos patvirtintas vadovėlis pedagoginių institutų matematikos specialybei

Scanned by Cloud Dancing

Vilnius „Mokslas" 1990

УДК 510(002)

Булота К., Сурвила П. Алгебра и теория чисел. Ч. 2: Учебник для студентов математических специальностей педагогических ин-тов. — 2-е изд., перераб. и доп. — Вильнюс: Мокслас, 1990. — 416 с., ил.

Во второй части учебника излагаются теория делимости целых чисел, цепные дроби, сравнения, сравнения с неизвестным и степенные вычеты, элементы теории колец и идеалов, общая теория многочленов. Отдельные разделы посвящены многочленам с числовыми коэффициентами и расширению оплей.

Ил. 4. Библиогр. 8 назв.

Leidinį recenzavo doc. **A. Matuliauskas**

В $\frac{1602040000-142}{M854(08)-90}$ **79—90**

ISBN 5-420-00613-8 (II d.)

ISBN 5-420-00416-X

© „Mokslo“ leidykla, 1977
© Kęstutis Bulota, Pranas Survila, 1990, pataisytas ir papildytas leidimas

Pratarmė

Antroji „Algebros ir skaičių teorijos" vadovėlio dalis, kaip ir pirmoji, skiriama pedagoginių institutų matematikos specialybės studentams. Ja taip pat galės naudotis kitų aukštųjų mokyklų studentai, studijuojantys matematiką. Manome, kad knyga bus naudinga ir matematikos mokytojams.

Šios vadovėlio dalies antrasis leidimas gerokai skiriasi nuo pirmojo. Pataisyti ar iš naujo parašyti kai kurie skyriai ir paragrafai, visai atsisakyta Galua teorijos pradmenų ir kai kurių dėsnių bei teoremų įrodymų, neįeinančių į algebros ir skaičių teorijos kurso programą. Iš dalies pakeista medžiagos pateikimo tvarka. Pirmiausia dėstomi tradiciniai skaičių teorijos klausimai: sveikųjų skaičių dalumo teorija, pirminiai skaičiai, grandininės trupmenos, lyginiai, po to – aukštosios algebros kurso dalis: žiedai ir idealai, polinomų teorija, laukų plėtiniai. Tokią dėstymo tvarką lėmė ilgametė autorių pedagoginio darbo patirtis – studentai žymiai lengviau įsisavina idealų teorijos pradmenis, kai jie pateikiami kaip tam tikri sveikųjų skaičių dalumo teorijos ir lyginių teorijos bendriniai. Dėl naujos dėstymo tvarkos teko žymiai keisti kai kurių teoremų įrodymus.

Knygoje paliesti ir į programą neįeinantys įdomesni skaičių teorijos klausimai, pateikta istorinio pobūdžio žinių, neišspręstų problemų. Tai padės plačiau susipažinti su šia įdomia ir sparčiai besivystančia matematikos šaka, kurios atstovų yra ir Lietuvoje.

Kaip ir pirmojoje vadovėlio dalyje, paragrafai ir teoremos numeruojami iš eilės, kiekvieno paragrafo pabaigoje pateikiama uždavinių.

Nuoširdžiai dėkojame docentams V. Bernotui ir R. Skrabutėnui, recenzentams doc. A. Matuliauskui ir doc. M. Makniui, nurodžiusiems pirmojo leidimo trūkumus ir pateikusiems daug vertingų pastabų ir patarimų.

Skaitytojams būsime dėkingi už kritines pastabas. Jas prašome siųsti „Mokslo" leidyklai (232050 Vilnius, Žvaigždžių 23) arba Vilniaus pedagoginio instituto Algebros ir skaičių teorijos katedrai (232034 Vilnius, Studentų 39).

Autoriai

Dalumo teorija sveikųjų skaičių žiede

§1. Sveikieji skaičiai ir jų veiksmai

Pagrindinis skaičių teorijos uždavinys – sveikojo skaičiaus savybių nagrinėjimas. Daugelis svarbių šios teorijos problemų tiesiogiai ar netiesiogiai susijusios su skaičiaus *dalumo* sąvoka. Todėl sveikųjų skaičių dalumo teorija užima svarbią vietą šiame algebros ir skaičių teorijos kurse.

Pirmojoje šio vadovėlio dalyje aptarėme pagrindines sveikųjų skaičių veiksmų savybes, nagrinėjome sveikųjų skaičių žiedus. Trumpai priminsime kai kurias sąvokas.

Sveikųjų skaičių aibę $\mathbf{Z}$ sudaro natūriniai skaičiai

$$1,\ 2,\ 3,\ \ldots,$$

neigiami sveikieji skaičiai

$$-1,\ -2,\ -3,\ \ldots$$

ir skaičius 0.

Natūrinius skaičius dar vadiname teigiamais sveikaisiais skaičiais. Teigiamus sveikuosius skaičius ir skaičių 0 vadiname *neneigiamais sveikaisiais skaičiais.*

Kiekvieną natūrinį skaičių n atitinka vienintelis neigiamas sveikasis skaičius $-n$. Skaičiai n ir $-n$ vadinami *priešingais sveikaisiais skaičiais.*

Sveikojo skaičiaus a *modulis* (absoliutinis didumas) $|a|$ apibrėžiamas šitaip:

$$|a| = \begin{cases} a, & \text{kai } a - \text{teigiamas sveikasis skaičius,} \\ 0, & \text{kai } a = 0, \\ -a, & \text{kai } a - \text{neigiamas sveikasis skaičius.} \end{cases}$$

Taigi sveikojo skaičiaus modulis – neneigiamas sveikasis skaičius. Nelygių nuliui sveikųjų skaičių moduliai yra natūriniai skaičiai.

Sveikųjų skaičių aibė sutvarkyta sąryšiu $<$ („mažiau“): nulis laikomas mažesniu už kiekvieną teigiamą sveikąjį skaičių, neigiamas sveikasis skaičius laikomas mažesniu už nulį. Iš dviejų neigiamų sveikųjų skaičių mažesnis tas, kurio modulis didesnis. Pavyzdžiui,

$$-100 < -2 < 0 < 2.$$

Jeigu a ir b yra sveikieji skaičiai, tai arba $a < b$, arba $a = b$, arba $b < a$ (*trichotomijos* savybė).

Kai $a<b$, skaičius a vadinamas mažesniu už skaičių b.

Ženklai $<$, $>$ gali būti vartojami kartu su lygybės ženklu. Užrašas $a\leqslant b$ reiškia, kad skaičius a arba mažesnis už b, arba jam lygus. Galima sakyti ir šitaip: a yra ne didesnis už b.

Pavyzdžiui, jeigu sveikasis skaičius $a\neq 0$, tai $|a|\geqslant 1$.

Pirmoje šio vadovėlio dalyje apibrėžėme kompleksinio skaičiaus modulį. Nesunku įsitikinti, kad kompleksinio skaičiaus modulio sąvoka sutampa su sveikojo skaičiaus modulio sąvoka, kai kompleksinis skaičius yra sveikasis skaičius a. Sveikąjį skaičių a užrašę $a+i0$ pavidalu, turime

$$\sqrt{a^2+0^2}=\sqrt{a^2}=|a|.$$

Gerai žinomas sveikųjų skaičių sudėties ir daugybos savybes galime išreikšti šitokiomis lygybėmis (jose raidės reiškia bet kokius sveikuosius skaičius):

1. $a+b=b+a$,

2. $a+(b+c)=(a+b)+c$,

3. $a+0=0+a=a$,

4. $a+(-a)=0$,

5. $a\,(bc)=(ab)c$,

6. $a\,(b+c)=ab+ac$,

7. $ab=ba$,

8. $|ab|=|a|\cdot|b|$.

Pirmoji ir septintoji savybės vadinamos atitinkamai sudėties ir daugybos *komutatyvumo* (perstatymo, keitimo) dėsniais, antroji ir penktoji – sudėties ir daugybos *asociatyvumo* (jungimo) dėsniais. Šeštoji savybė – sudėties ir daugybos veiksmus siejantis *distributyvumo* (skirstymo) dėsnis. Aštuntoji lygybė reiškia trivialią, bet svarbią modulio savybę.

Šios bei kitos iš jų išplaukiančios sveikųjų skaičių veiksmų savybės buvo aptartos vadovėlio I dalyje nagrinėjant sveikųjų skaičių žiedą – struktūrą $(\mathbf{Z},\ +,\ \cdot)$.

Paminėsime dar dvi sveikųjų skaičių aibės savybes, kuriomis vėliau teks remtis.

Mažiausiojo skaičiaus principai. *Kiekviename netuščiame natūrinių skaičių aibės poaibyje yra mažiausias elementas.*

Kiekviename netuščiame baigtiniame sveikųjų skaičių aibės poaibyje yra mažiausias elementas.

Didžiausiojo skaičiaus principas. *Kiekviename netuščiame baigtiniame sveikųjų skaičių aibės poaibyje yra didžiausias elementas.*

Sveikųjų ir natūrinių skaičių aibės turi daug bendrų savybių: jos yra begalinės, suskaičiuojamos (skaičios), sutvarkytos, diskrečios (primename, jog pastaroji savybė reiškia štai ką: paėmę bet kurį aibės elementą, galime rasti artimiausią kaimyninį (gretimą) elementą). Vienas iš svarbesnių sveikųjų ir natūrinių skaičių aibių skirtumų – natūrinių skaičių aibėje yra mažiausias elementas 1, o sveikųjų skaičių aibėje mažiausio elemento nėra ir ji neribotai tęsiasi į abi puses:

$$\ldots,\ -n,\ \ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots,\ n,\ \ldots$$

Šiame skyriuje sveikuosius skaičius dažniausiai žymėsime mažosiomis raidėmis, tik kai kuriose formulėse, sekdami istorine tradicija, jiems žymėti vartosime didžiąsias raides. Bet kuri mažoji lotyniška raidė, jei nebus kitaip nurodyta, reikš sveikąjį skaičių. Natūrinius skaičius dažniausiai žymėsime raide n.

§2. Dalumo sąryšis sveikųjų skaičių žiede ir jo savybės

Sveikųjų skaičių aibė nėra uždara daugybai atvirkštinio veiksmo — dalybos — atžvilgiu, todėl šiai operacijai skirsime daugiau dėmesio negu kitoms trims. Nagrinėsime dalybą sveikųjų skaičių žiede.

Sakome, kad sveikasis skaičius a dalijasi iš sveikojo skaičiaus $b\neq 0$, jeigu yra toks sveikasis skaičius c, kad $a=bc$. Tuo atveju rašome $b \mid a$.

Statųjį brūkšnelį $\mid$ išraiškoje $b \mid a$ vadinsime *dalumo ženklu*. Matematinėje literatūroje galima rasti ir kitokių dalumo ženklų, pavyzdžiui, $\backslash$, $\vdots$, $/$.

Jeigu $b \mid a$ ir $a=bc$, tai skaičių b vadinsime skaičiaus a *dalikliu*, a — skaičiaus b *kartotiniu*, c — skaičių a ir b *dalmeniu* arba *skaičiaus b papildomuoju dalikliu*. Skaičių c galime užrašyti trejopai:

$$c=a:b=\frac{a}{b}=a/b. \tag{1.1}$$

Lygybės $a=bc$ dešinėje pusėje esančius skaičius b ir c galime sukeisti vietomis, todėl ir skaičių c galime vadinti skaičiaus a dalikliu, o b — jo papildomuoju dalikliu.

Užrašą $b \mid a$ galime skaityti ir šitaip:

b *dalija* a,

a *dalijasi iš* b.

Jeigu a nesidalija iš b, rašome $b \nmid a$.

Kadangi, kai $a\neq 0$, joks skaičius x netenkina lygybės $0\cdot x=a$, tai užrašas $a:0$ yra neapibrėžtas. Todėl iš nulio dalyti negalima. Sutarsime, kad $b \mid a$ pavidalo išraiškose į kairę nuo dalumo ženklo esantis skaičius b niekada negali būti lygus 0, ir kiekvienu atskiru atveju to nepriminsime.

Akivaizdžios šios dalumo savybės:

$$1 \mid a, \quad a \mid a, \quad a \mid 0, \tag{1.2}$$

t. y. kiekvienas nelygus nuliui sveikasis skaičius a dalijasi iš vieneto bei pats iš savęs, o nulis dalijasi iš bet kurio sveikojo skaičiaus $a\neq 0$.

Išvardysime ir kitas, kiek sudėtingesnes, tačiau lengvai iš dalumo apibrėžimo gaunamas savybes.

1. *Jeigu* $b \mid a$, *tai* $\pm b \mid \pm a$.
2. *Jeigu* $b \mid a$, *tai* $kb \mid ka$ $(k \neq 0,\ k \in \mathbf{Z})$.
3. *Jeigu* $kb \mid ka$, *tai* $b \mid a$.
4. *Jeigu* $b \mid a$, *tai* $b \mid ak$ $(k \in Z)$.
5. *Jeigu* $c \mid b$ *ir* $b \mid a$, *tai* $c \mid a$.

Visos šios savybės įrodomos gana paprastai. Įrodysime, pavyzdžiui, trečiąją savybę.

Tarkime, kad $kb \mid ka$. Tai reiškia, kad yra toks sveikasis skaičius c, su kuriuo

$$ka = kbc.$$

Kadangi $k \neq 0$, tai šios lygybės abi puses galime padalyti iš k. Padaliję gaunam $a = bc$. Ši lygybė ir reiškia, kad $b \mid a$.

5 dalumo savybė kartais vadinama *dalumo tranzityvumo* savybe.

Suformuluosime dar tris mažiau akivaizdžias savybes, kurios labai praverčia sprendžiant kai kuriuos skaičių teorijos uždavinius.

6. *Jeigu* $b \mid a$ *ir* $b \mid c$, *tai* $b \mid (a \pm c)$.
7. *Jeigu* $b \mid a$ *ir* $d \mid c$, *tai* $bd \mid ac$.
8. *Jeigu* $b \mid a$ ir $n \in \mathbf{N}$, *tai* $b^n \mid a^n$.

Įrodysime pirmąją iš tų trijų savybių, kitas paliksime įrodyti skaitytojui.

Jeigu $b \mid a$, tai yra toks sveikasis skaičius k, su kuriuo

$$a = bk.$$

Analogiškai, jeigu $b \mid c$, tai yra toks sveikasis skaičius t, su kuriuo

$$c = bt.$$

Sudėję (atėmę) panariui šias lygybes, gausime

$$a \pm c = b(k \pm t).$$

Suma $k+t$ (skirtumas $k-t$) yra sveikasis skaičius, todėl pagal dalumo apibrėžimą pastaroji lygybė ekvivalenti teiginiui $b \mid (a+c)$ (teiginiui $b \mid (a-c)$).

6 ir 7 savybės lengvai apibendrinamos didesniam dėmenų (atitinkamai dauginamųjų) skaičiui.

Atrodytų, kad nėra labai sudėtinga rasti kokį nors skaičiaus a daliklį (savaime aišku, nelygų ± 1 arba $\pm a$). Tačiau, kai a didelis skaičius, tai jau — problema. Kartais net nelengva atsakyti į klausimą, ar apskritai yra tokių daliklių. Plačiai žinomas prancūzų matematiko *Pjero Ferma* (P. Fermat, 1601—1665) klaidingas tvirtinimas, kad skaičius $a = 4\,294\,967\,297$ neturi daliklių d, $1 < d < a$. Šimtmečiu vėliau Leonardas Oileris įrodė, kad tas skaičius dalijasi iš 641. Galima būtų manyti, kad tai — praeitų amžių problemos, o dabar, turint šiuolaikinę skaičiavimo techniką, tokių klausimų nekyla. Deja, ne visai taip. Štai, pavyzdžiui, 1964 m. matematikams buvo žinoma, kad skaičius $a = 2^{101} - 1$ turi du daliklius d, $1 < d < a$, bet nebuvo žinoma, kaip juos rasti.

Galingi kompiuteriai padėjo atsakyti į kai kuriuos dalumo klausimus. Pavyzdžiui, buvo nustatyta, kad skaičius $2^{65536} - 1$, turintis 19 729 skaitmenų, dalijasi iš skaičiaus 825 753 601, o skaičius $18! - 1$ turi 5 natūrinius daliklius, tarp kurių yra ir šie: 59, 22 663, 478 749 547. Būtų sunkoka trumpai išaiškinti, kuo minėtieji skaičiai ar jų dalikliai nusipelnė tokio dėmesio. Tačiau manytume, kad daliklių problemos, kaip ir kiti skaičių teorijos ar algebros klausimai, galėtų būti įdomios tiek matematikos mokytojui, tiek ir jo mokiniams.

Uždaviniai

Įrodykite šias sveikųjų skaičių modulio savybes:

1. $|a+b| \leqslant |a|+|b|$,

2. $|a-b| \geqslant |a|-|b|$.

Su kuriais sveikaisiais skaičiais x teisingos šios lygybės:

3. $|x-1|=|x|$,

4. $||x|-4|=3|x|$?

5. Raskite sandaugos $-16 \sin 10^\circ \cos 20^\circ \sin 50^\circ$ modulį.

6. Įrodykite: jeigu $b \mid a$, tai skaičiaus b papildomasis daliklis randamas vienareikšmiškai.

7. Įrodykite dalumo savybę: jeigu $b \mid a$, $c \mid b$, $d \mid c$, tai $d \mid a$.

8. Nustatykite, kokia išvada išplaukia iš to, kad $b \mid a$ ir kartu $a \mid b$.

9. Įrodykite 1–2, 4–5, 7–8 dalumo savybes.

10. Įrodykite: jeigu $mn+pq$ dalijasi iš $m-p$, tai ir $mq+np$ dalijasi iš $m-p$.

11. Įrodykite, kad sandauga $n(n+1)(2n+1)$ dalijasi iš 6 (n – natūrinis skaičius).

§3. Dalikliai ir kartotiniai

Iš dalumo savybių išplaukia, kad bet kuris sveikasis skaičius a, kai $|a|>1$, turi mažiausiai 4 daliklius: 1, -1, a, $-a$. Suprantama, šie dalikliai neteikia jokios naudingos informacijos. Juos vadinsime *trivialiaisiais dalikliais.*

Taip pat minėjome, kad skaičiui b priešingas skaičius $-b$ yra skaičiaus a daliklis, jeigu b yra a daliklis. Todėl visus sveikojo skaičiaus a daliklius galime sugrupuoti į teigiamuosius ir neigiamuosius daliklius. Šios daliklių aibės skiriasi tik elementų ženklais. Todėl sprendžiant teorinius ir praktinius uždavinius, pakanka rasti vien teigiamuosius daliklius. Toliau žodžiu „daliklis“ vadinsime tik teigiamąjį daliklį. Pavyzdžiui, sakysime, kad visi skirtingi skaičiaus -15 dalikliai yra 1, 3, 5, 15.

Kalbėdami apie skaičiaus a trivialiuosius daliklius taip pat turėsime omenyje jo trivialiuosius teigiamus daliklius.

Netrivialieji skaičiaus a dalikliai tenkina sąlygą

$$1 < d < |a|.$$

Iš šios nelygybės išplaukia, kad kiekvienas skaičius a turi tik baigtinį skaičių daliklių. Tačiau bendruoju atveju visus juos rasti žymiai sunkiau negu apibūdinti skaičiaus a kartotinius, nors pastarųjų be galo daug. Pavyzdžiui, nesunkiai galime užrašyti skaičiaus 2^{128} daliklius:

$$1,\ 2,\ 2^2,\ 2^3,\ 2^4,\ \ldots,\ 2^{127},\ 2^{128}.$$

O apie skaičiaus $2^{128}+1$ netrivialiuosius daliklius žinome tik tiek, kad jų yra ne mažiau kaip 3. Sunku aptikti kokius nors daliklių paieškų dėsningumus.

Papildomųjų daliklių radimas problemų nekelia. Akivaizdus toks sąryšis:

$$d \mid a \Leftrightarrow \frac{a}{d} \mid a.$$

Beje, jeigu vienoje eilutėje išrašytume visus skaičiaus a daliklius, kitoje eilutėje – pastarųjų papildomuosius daliklius, tai abiejose eilutėse būtų surašyti tie patys skaičiai, tik priešinga tvarka.

Pavyzdžiui, skaičiaus $a=36$ dalikliai ir jų papildomieji dalikliai yra šie:

$$1,\ 2,\ 3,\ 4,\ 6,\ 9,\ 12,\ 18,\ 36,$$

$$36,\ 18,\ 12,\ 9,\ 6,\ 4,\ 3,\ 2,\ 1.$$

Matome, kad radę skaičiaus 36 daliklius, ne didesnius už 6, ir tų daliklių papildomuosius daliklius, gauname visus to skaičiaus daliklius. Skaičius 6 lygus kvadratinei šakniai iš 36. Panašiai būtų ir imant bet kokį kitą skaičių. Taigi ieškant skaičiaus a visų daliklių, reikia rasti jo daliklius $d \leqslant \sqrt{|a|}$ ir pastarųjų papildomuosius daliklius.

Iš dalumo savybių išplaukia, kad kiekvienas sveikasis skaičius $b \neq 0$ turi be galo daug kartotinių – jo kartotiniai yra visi bk pavidalo skaičiai. Skaičiaus b kartotinių eilė

$$\ldots,\ -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b,\ \ldots$$

begalinė į abi puses. Todėl nėra prasmės ieškoti visų kurio nors skaičiaus kartotinių, jeigu jų neriboja papildomos sąlygos.

Apibrėšime dvi svarbias funkcijas, susijusias su skaičiaus kartotiniais tam tikrame intervale.

Realiojo skaičiaus x sveikąja dalimi vadiname didžiausią sveikąjį skaičių, ne didesnį už x.

Skaičiaus x sveikoji dalis dažniausiai žymima $[x]$. Ta funkcija dažnai dar vadinama *antje x* (prancūzų k. žodis *entier* reiškia matematikoje „sveikas“; iš čia ir kitas žymėjimas – $E(x)$).

Iš apibrėžimo išplaukia, kad teisinga nelygybė

$$[x] \leqslant x < [x] + 1. \tag{1.3}$$

Ši nelygybė taip pat gali būti skaičiaus x sveikosios dalies apibrėžimu.

Skirtumas $x-[x]$ vadinamas skaičiaus x *trupmenine dalimi* ir žymimas $\{x\}$. Vadinasi,

$$x = [x] + \{x\}.$$

Iš skaičiaus sveikosios dalies apibrėžimo išplaukia, kad $\{x\} \geqslant 0$. Jeigu x yra sveikasis skaičius, tai $[x]=x$, $\{x\}=0$. Pavyzdžiui,

$$[2{,}5]=2,\ [\pi]=3,\ \left[-1\tfrac{1}{3}\right]=-2,\ [2^5]=2^5,$$

$$[2^{-5}]=0,\ \{2^{-5}\}=2^{-5},\ \{\pi\}=0{,}1415\ldots$$

Nagrinėsime, kiek yra natūrinio skaičiaus d kartotinių tam tikrame intervale.

1 teorema. *Yra $\frac{x}{d}$ natūrinių skaičiaus d kartotinių, ne didesnių už x ($x>0$).*

Įrodymas. Natūriniai skaičiaus d kartotiniai yra

$$d,\ 2d,\ 3d,\ \ldots$$

Jeigu md – paskutinis iš tų kartotinių, ne didesnių už x, tai

$$md \leqslant x < (m+1)d.$$

Iš čia

$$m \leqslant \frac{x}{d} < m+1.$$

Palyginę pastarąją nelygybę su skaičiaus sveikosios dalies (1.3) apibrėžimu, matome, kad

$$m = \left[\frac{x}{d}\right].$$

Taigi teorema įrodyta.

Pavyzdys. Iš 13 dalijasi 7 natūriniai skaičiai, ne didesni už 100, nes

$$\left[\frac{100}{13}\right] = 7.$$

Išvada. Jeigu $x > 0$, tai

$$\left[\frac{[x]}{d}\right] = \left[\frac{x}{d}\right]. \tag{1.4}$$

Įrodymas. Tarp $[x]$ ir x sveikųjų skaičių nėra, todėl skaičiaus d natūrinių kartotinių, ne didesnių už $[x]$, yra tiek pat, kiek yra kartotinių, ne didesnių už x.

Atkreipsime dėmesį, kad iš sveikosios dalies (1.3) apibrėžimo išplaukia šitoks priešingų skaičių sveikųjų dalių sąryšis:

$$\{x\} \neq 0 \Leftrightarrow [-x] = -[x] - 1.$$

Uždaviniai

12. Raskite visus skaičių 240, 300, 650, 720 daliklius.

13. Raskite skaičių -96, 420, -270, 1050 netrivialiuosius daliklius ir pastarųjų papildomuosius.

14. Nustatykite, ar skaičiai $12+12!+13!+14!$, $121+121!$, $2^{16}3^75^8+3^{17}5^87^9+2^65^87^7+2^95^87^4+2^{11}3^47^{11}$ turi netrivialiųjų vienaženklių daliklių.

15. Raskite šių skaičių sveikąsias dalis:

a) $(-0{,}027)^{(-1{,}5)^{-1}}$; b) $(\sin 15°)^{-1}$; c) $\log_2 \log_2 \log_2 256$.

16. Raskite šių skaičių sveikąsias dalis:

a) $-\pi$; b) -2^{-2}; c) e^3; d) $\operatorname{tg} \frac{\pi}{3}$.

17. Raskite šių skaičių sveikąsias dalis:

a) $(\sqrt{2}-\sqrt{3})^3$; b) $(\sqrt{2}-\sqrt{3})^{-3}$; c) $\left((1+3^{-1/2})^{-1}\right)^{-2}$.

18. Raskite šių skaičių trupmenines dalis:

a) $-\frac{1}{3}-\frac{1}{9}-\frac{1}{27}-\ldots$; b) $-\operatorname{tg}\frac{\pi}{4}+\frac{1}{4}$; c) $(-\log_2 \sqrt[5]{64})^2$.

19. Nustatykite, kiek skaičių n, $25 \leqslant n \leqslant 200$, nesidalija iš 7.

20. Kurios iš šių lygčių išsprendžiamos su realiaisiais skaičiais x:
a) $16[x]^2=9$; b) $[x]=\pi$; c) $[x]+[x]^2=6$; d) $2[x]+7=-2\{x\}$?
Raskite jų sprendinius.

21. Kiek triženklių skaičių dalijasi iš 13?

§4. Dalybos su liekana teorema. Euklido algoritmas

Sveikųjų skaičių dalumo teorijoje labai svarbi ši teorema.

2 (dalybos su liekana) teorema. *Imant bet kurią sveikųjų skaičių a ir $b\neq 0$ porą, galima rasti tokią vienintelę sveikųjų skaičių q ir r porą, su kuria būtų teisinga lygybė*

$$a=bq+r, \quad 0\leqslant r<|b|. \tag{1.5}$$

I įrodymas. Pakanka nagrinėti atvejį, kai $b>0$. Jeigu $b \mid a$, tai (1.5) lygybė teisinga pagal dalumo apibrėžimą (tuo atveju $r=0$). Jeigu $b\nmid a$, tai a nėra b kartotinis.

Tarkime, kad $a>0$. Sudarykime skaičiaus b kartotinių eilę

$$b\cdot 1,\ b\cdot 2,\ b\cdot 3,\ \ldots \tag{1.6}$$

Pažymėkime raide M aibę tų b kartotinių, kurie didesni už a. Pagal mažiausio skaičiaus principą aibėje M yra mažiausias elementas, kurį žymėkime bs'. Raide s žymėkime skaičių, kuris vienetu mažesnis už s'. Taigi $s+1=s'$. Akivaizdi nelygybė

$$bs\leqslant a<b(s+1).$$

Nagrinėsime atvejį, kai $a<0$, arba $-a>0$. Aibę M galime sudaryti iš tokių (1.6) pavidalo skaičių, kurie yra ne mažesni už $-a$. Pagal mažiausiojo skaičiaus principą ir šiuo atveju aibėje M yra mažiausias elementas, sakykim, bt'. Tuomet teisinga nelygybė

$$bt<-a\leqslant b(t+1),$$

kurioje $t=t'-1$. Vadinasi, $b(-t-1)\leqslant a<b(-t)$.

Matome, kad tiek vienu, tiek kitu atveju egzistuoja toks sveikasis skaičius q, su kuriuo teisinga nelygybė

$$bq\leqslant a<b(q+1).$$

Iš čia, pažymėję raide r skirtumą $a-bq$, gauname

$$0\leqslant r=a-bq<b(q+1)-bq=b.$$

Taigi gavome teoremos formuluotėje pateiktą (1.5) nelygybę, kurioje r tenkina nurodytas sąlygas.

Jeigu b neigiamas, tai pakanka užrašyti įrodytąją lygybę skaičiams a ir $-b$, po to atitinkamai pakeisti q ir $-b$ ženklus.

Tarę, kad, be išraiškos $a=bq+r$, galima rasti išraišką su kita pora q' ir r', t. y. kad $a=bq'+r'$, $0\leqslant r'<b$, nesunkiai įsitikinsime, kad būtinai $q=q'$ ir $r=r'$. Tai įrodyti siūlome skaitytojui.

Šis teoremos įrodymas paremtas mažiausiojo skaičiaus principu. Pateiksime ir kitą įrodymą, paremtą žinomomis sveikųjų skaičių aibės sutvarkymo savybėmis.

II įrodymas. Kaip ir pirmajame įrodyme, apsiribosime atveju, kai $b>0$. Natūrinio skaičiaus b kartotinių eilė neribotai tęsiasi į abi skaičių tiesės puses:

$$\ldots < -3b < -2b < -b < 0 < b < 2b < 3b < \ldots$$

Sveikasis skaičius a arba yra b kartotinis qb (tuo atveju (1.5) lygybė teisinga, joje $r=0$), arba jį galima vienintelių būdu įterpti tarp kažkurių dviejų gretimų skaičiaus b kartotinių:

$$bq < a < b(q+1).$$

Pažymėję $r=a-bq$, iš anksčiau parašytų nelygybių gauname teisingą nelygybę $0 \leqslant r \leqslant b$ bei lygybę $a=bq+r$. Akivaizdu, kad q ir r randami vienareikšmiškai.

Atvejis, kai $b<0$, aptariamas panašiai kaip ir I įrodyme. Teorema įrodyta.

Pavyzdžiai. 1. Jeigu $a=100$, $b=12$, tai $q=8$ ir $r=100-8\cdot 12=4$. Taigi

$$100=12\cdot 8+4.$$

2. Jeigu $a=-1$, $b=13$, tai $q=-1$, $r=-1-(13)(-1)=12$, nes $-13<-1<0$. Todėl

$$-1=13\cdot(-1)+12.$$

Jeigu $a=bq+r$ $(0 \leqslant r < b)$, tai sakome, kad skaičius *a padalytas iš skaičiaus b su liekana.* Skaičius q vadinamas skaičių a ir b *dalybos nepilnuoju santykiu (nepilnuoju dalmeniu),* r vadinamas skaičiaus a dalybos iš skaičiaus b *liekana.*

Palyginę ankstesnę nelygybę $[x] \leqslant x < [x]+1$ su nelygybe $bq \leqslant a < b(q+1)$, matome, kad skaičių a ir b nepilnasis santykis yra skaičiaus a/b sveikoji dalis:

$$q=\left[\frac{a}{b}\right].$$

Taigi skaičių a ir b nepilnasis santykis q skiriasi nuo jų tikrojo santykio (racionaliojo skaičiaus a/b) teigiamu dydžiu, mažesniu už 1.

Euklido algoritmas. Dalybos su liekana teorema pagrįstas vadinamasis *Euklido algoritmas.*

Euklido algoritmu vadinamas nuoseklus dalybos su liekana teoremos taikymas: pirmiausia žinomų skaičių a ir b porai, po to skaičių b ir r (r yra a dalybos iš b liekana) porai, toliau — skaičių r ir r_1 (r_1 — b dalybos iš r liekana) porai ir t. t. Procesas tęsiamas tol, kol gaunama liekana $r_{k+1}=0$:

$$\begin{aligned}
a &= bq + r, && 0 < r < |b|,\\
b &= rq_1 + r_1 && 0 < r_1 < r,\\
r &= r_1 q_2 + r_2, && 0 < r_2 < r_1,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{k-2} &= r_{k-1} q_k + r_k, && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k q_{k+1}.
\end{aligned} \tag{1.7}$$

Sakome, kad Euklido algoritmą pritaikėme skaičių a ir b porai.

Iš šių nelygybių matome, kad liekanos r, r_i (jas vadinsime algoritmo liekanomis) nuosekliai mažėja. Kadangi jos yra neneigiami sveikieji skaičiai,

tai būtinai po baigtinio žingsnių skaičiaus (ne didesnio už $|b|$) dalybos procesas nutrūks: būtent tada, kai gausime liekaną, lygią 0.

Taikant Euklido algoritmą, neretai prireikia išreikšti algoritmo liekanas r_i pradiniais skaičiais a, b bei nepilnaisiais santykiais q_i. Šis darbas labai palengvėja pasinaudojus vadinamaisiais *Oilerio skliaustais.*

Oilerio skliaustai (čia juos žymėsime dvigubais lenktiniais skliaustais, kitur jie gali būti žymimi ir kitaip) apibrėžiami šitokiomis rekurentinėmis formulėmis:

$$((k_1)) = k_1,$$

$$((k_1,\ k_2)) = k_1 k_2 + 1,$$

$$((k_1,\ k_2,\ \ldots,\ k_{n-1},\ k_n,\ k_{n+1})) = ((k_1,\ k_2,\ \ldots,\ k_{n-1},\ k_n))\,k_{n+1} + ((k_1,\ k_2,\ \ldots,\ k_{n-1})),\quad n \geqslant 2. \tag{1.8}$$

(Plačiau apie Oilerio skliaustus skaitykite šio vadovėlio I leidime.)

Pavyzdžiui, $((3,\ 2,\ 4)) = ((3,\ 2)) \cdot 4 + ((3)) = (3 \cdot 2 + 1) \cdot 4 + 3 = 31$.

Nesunku įrodyti, kad Euklido algoritmo (1.7) liekana r_s $(1 \leqslant s \leqslant k)$ gali būti išreikšta šitaip:

$$r_s = (-1)^s a \cdot ((q_1,\ q_2,\ \ldots,\ q_s)) + (-1)^{s+1} b \cdot ((q,\ q_1,\ q_2,\ \ldots,\ q_s)). \tag{1.9}$$

Įrodysime naudodamiesi sustiprintuoju pilnosios matematinės indukcijos principu. Kai $s=1$, (1.9) formulė yra šitokia:

$$r_1 = -a((q_1)) + b((q,\ q_1)) = -q_1 a + (qq_1 + 1)b.$$

Kad ji teisinga, lengvai išplaukia iš Euklido algoritmo (1.7) pirmųjų dviejų lygybių. Tarkime, kad (1.9) formulė teisinga su visais j, $1 \leqslant j \leqslant s-1$. Tuomet iš atitinkamos Euklido algoritmo lygybės

$$r_{s-2} = r_{s-1} q_s + r_s$$

gauname:

$$r_s = r_{s-2} - r_{s-1} q_s = (-1)^{s-2} a \cdot ((q_1,\ q_2,\ \ldots,\ q_{s-2})) + (-1)^{s-1} b \cdot ((q,\ q_1,\ q_2,\ \ldots,\ q_{s-2})) - (-1)^{s-1} a \cdot ((q_1,\ q_2,\ \ldots,\ q_{s-1}))\cdot q_s - (-1)^s b \cdot ((q,\ q_1,\ q_2,\ \ldots,\ q_{s-1}))\cdot q_s.$$

Sugrupavę koeficientus prie a ir prie b, įsitikiname, kad (1.9) formulė teisinga ir kai $j=s$. Taigi ši formulė įrodyta.

Skaičiavimai pagal (1.9) formulę žymiai supaprastėja, jei Oilerio skliaustų reikšmių ieškoma naudojantis tam tikra lentele, kurią toliau ir aptarsime.

Imkime, pavyzdžiui, skaičius $a=13444$, $b=1326$ ir užrašykime Euklido algoritmo lygybes:

$$13444 = 1326 \cdot 10 + 184,$$

$$1326 = 184 \cdot 7 + 38,$$

$$184 = 38 \cdot 4 + 32,$$

$$38 = 32 \cdot 1 + 6,$$
$$32 = 6 \cdot 5 + 2,$$
$$6 = 2 \cdot 3.$$

Sudarykime lentelę, kurios pirmojoje eilutėje surašykime nepilnuosius santykius q_l, o antrojoje ir trečiojoje eilutėse – atitinkamas Oilerio skliaustų reikšmes:

q_l	10	7	4	1	5
$((q, q_1, \ldots, q_l))$	10	71	294	365	2119
$((q_1, \ldots, q_l))$		7	29	36	209

Antrojoje ir trečiojoje eilutėse pirmasis skaičius lygus atitinkamam q_l. Tai atitinka Oilerio skliaustų (1.8) apibrėžimo pirmąją lygybę. Antrasis skaičius kiekvienoje iš tų eilučių gaunamas pirmąjį eilutės skaičių padauginus iš tolesniame stulpelyje parašyto q_l ir prie gautos sandaugos pridėjus 1. Tai atitinka 2-ąją (1.8) apibrėžimo eilutę. Kiekvienas tolesnis antrosios ir trečiosios eilučių skaičius randamas paskutinį atitinkamos eilutės skaičių padauginus iš paskesniame stulpelyje parašyto q_l ir prie gautos sandaugos pridėjus prieš-paskutinį parašytą tos eilutės skaičių. Pavyzdžiui, antrojoje eilutėje skaičius 294 gautas skaičių 71 padauginus iš paskesniame stulpelyje parašyto $q_3 = 4$ ir prie gautos sandaugos pridėjus skaičių 10.

Naudodamiesi tokia lentele ir remdamiesi (1.9) formule, visas skaičiams 13444 ir 1326 pritaikyto Euklido algoritmo liekanas galime išreikšti tais skaičiais ir nepilnaisiais santykiais:

$$r_4 = 2 = 13444 \cdot 209 - 1326 \cdot 2119,$$
$$r_3 = 6 = -13444 \cdot 36 + 1326 \cdot 365,$$
$$r_2 = 32 = 13444 \cdot 29 - 1326 \cdot 294,$$
$$r_1 = 38 = -13444 \cdot 7 + 1326 \cdot 71.$$

Toliau nagrinėkime atvejį, kai vietoje skaičiaus $b = 1326$ paimtas priešingas skaičius $b = -1326$. Taikydami Euklido algoritmą, gauname šitokias lygybes:

$$13444 = (-1326) \cdot (-10) + 184,$$
$$-1326 = 184 \cdot (-8) + 146,$$
$$184 = 146 \cdot 1 + 38,$$
$$146 = 38 \cdot 3 + 32,$$
$$38 = 32 \cdot 1 + 6,$$
$$32 = 6 \cdot 5 + 2,$$
$$6 = 2 \cdot 3.$$

Oilerio skliaustams apskaičiuoti sudarome atitinkamą lentelę:

q_i	-10	-8	1	3	1	5
$((q, q_1, q_2, \ldots, q_i))$	-10	81	71	294	365	2119
$((q_1, q_2, \ldots, q_i))$		-8	-7	-29	-36	-209

Iš šios lentelės galime išreikšti skaičių 13444 ir -1326 Euklido algoritmo liekanas (dabar jų numeracija neatitinka pirmojo atvejo numeracijos, nes šiuo atveju algoritmas ilgesnis):

$$r_5 = 2 = -13444 \cdot (-209) + (-1326) \cdot 2119,$$
$$r_4 = 6 = 13444 \cdot (-36) - (-1326) \cdot 365,$$
$$r_3 = 32 = -13444 \cdot (-29) + (-1326) \cdot 294,$$
$$r_2 = 38 = 13444 \cdot (-7) - (-1326) \cdot 71,$$
$$r_1 = 146 = -13444 \cdot (-8) + (-1326) \cdot 81.$$

Uždaviniai

22. Įrodykite dalybos su liekana teoremos vienatį (tarę, kad žinomų skaičių a ir b porai galima rasti dvi skirtingas poras q_1, r_1 ir q_2, r_2, gaukite prieštaravimą).

23. Pritaikykite Euklido algoritmą šioms skaičių poroms:
a) -28 ir 39; b) 13 ir 8; c) -64 ir 57.

24. Pritaikykite Euklido algoritmą šioms skaičių poroms:
a) 972 ir -421; b) -3001 ir -179; c) 10 012 ir 920.

25. Pritaikykite Euklido algoritmą skaičių a ir b porai, kai algoritmas yra 6 eilučių ($r_6 = 0$), ir išreikškite liekanas r_3 ir r_4 skaičiais a, b bei nepilnaisiais santykiais q_i.

26. Pritaikykite Euklido algoritmą skaičiams 720 ir -47; išreikškite visas algoritmo liekanas r_i tais skaičiais ir atitinkamais nepilnaisiais santykiais remdamiesi (1.9) formule.

§5. Skaičiavimo sistemos

Bet kurį dešimtainiais skaitmenimis užrašytą skaičių visame pasaulyje vienodai supras. Pavyzdžiui, skaičius 15 147 reiškia sumą

$$10^4 + 5 \cdot 10^3 + 1 \cdot 10^2 + 4 \cdot 10 + 7.$$

Iš dešinės į kairę to skaičiaus skaitmenys yra ne kas kita, kaip koeficientai prie nuosekliai didėjančių 10 laipsnių, visi jie mažesni už 10. Skaičius 10 yra mūsų įprastinės skaičiavimo sistemos pagrindas, pati ta sistema vadinama *dešimtaine*. Skaičiaus, užrašyto dešimtainėje skaičiavimo sistemoje, skaitmenis rašome greta:

$$N = \sum_{i=0}^{k} a_i 10^i = \overline{a_k a_{k-1} \ldots a_1 a_0}.$$

Dešimtainė skaičiavimo sistema nėra vienintelė ir patogiausia. Tik dėl tūkstantmetės tradicijos ta sistema yra dominuojanti.

Pastaruoju metu vis plačiau vartojamos ir kitos skaičiavimo sistemos. Pavyzdžiui, skaičiavimo technikoje dvejetainė (kartais aštuonetainė) sistema žymiai patogesnė už dešimtainę. Susipažinsime su kai kuriais skaičiavimo sistemų dėsniais.

Skaičius, užrašytus skaičiavimo sistemoje, kurios pagrindas $g>1$, vadinsime sisteminiais skaičiais.

Užrašant skaičių sistemoje, kurios pagrindas yra g, laikomasi tų pačių dėsnių kaip ir dešimtainėje sistemoje: skaičius taip išreiškiamas skirtingų skaičiaus g neneigiamų laipsnių suma, kad koeficientai prie tų laipsnių būtų ne didesni už $g-1$. Pavyzdžiui, užrašykime skaičių 613 šešetainėje skaičiavimo sistemoje:

$$613=2\cdot 6^3+5\cdot 6^2+0\cdot 6+1=\overline{2501}_{(6)}.$$

Indeksas (6) (kartais jį rašysime be skliaustų) rodo, kad skaitmenys 2, 5, 0, 1 reiškia ne skaičių, lygų dviem tūkstančiams penkiems šimtams vienam, bet koeficientus prie 6 laipsnių – skaičiaus užrašo šešetainėje sistemoje skaitmenis.

Įrodysime, kad, parinkus bet kokį natūrinį sistemos pagrindą $g>1$, kiekvienas skaičius toje sistemoje užrašomas vienareikšmiškai.

3 teorema. *Kiekvienas natūrinis skaičius a vieninteliu būdu užrašomas kaip sisteminis skaičius sistemoje, kurios pagrindas yra $g>1$:*

$$a=b_k g^k+b_{k-1}g^{k-1}+\ldots+b_2 g^2+b_1 g+b_0; \qquad (1.10)$$

čia b_i – neneigiami sveikieji skaičiai, mažesni už g, $k\geqslant 0$, $b_k\geqslant 0$.

Įrodymas. Įrodysime matematinės indukcijos metodu.

Jeigu $a=1$, tai trivialiai $0<b_0=1<g$, $k=0$. Šiuo atveju teorema teisinga. Tarkime, kad visi skaičiai, mažesni už n, užrašomi vienareikšmiškai (1.10) pavidalu. Įrodysime, kad taip galima užrašyti ir skaičių n. Padalysime n iš g su liekana:

$$n=qg+b_0,\ 0\leqslant b_0<g. \qquad (1.11)$$

Skaičius $q<n$ ir todėl pagal prielaidą užrašomas (1.10) pavidalu:

$$q=b_k g^{k-1}+b_{k-1}g^{k-2}+\ldots+b_2 g+b_1\ \ (0\leqslant b_i<g,\ b_k>0).$$

q išraiškoje koeficientų indeksą specialiai rašėme vienetu didesnį už g laipsnį. Įrašę tą išraišką į (1.11) lygybę, gauname skaičiaus n (1.10) pavidalo išraišką. Skaičiaus (1.10) išraiškos vienatis išplaukia iš to, kad dalybos su liekana teoremoje (2 teorema) nepilnasis santykis ir liekana randami vienareikšmiškai.

Teorema įrodyta.

Aritmetiniai veiksmai su sisteminiais skaičiais atliekami pagal tas pačias taisykles kaip ir veiksmai su dešimtainiais skaičiais. Išnagrinėsime, pavyzdžiui, dešimtainių skaičių sudėtį. Kiekviename sudėties etape galima dvejopa situacija:

$$\begin{array}{r} **cb** \\ \hline **cd** \end{array} \quad \begin{array}{l} \\ a** \end{array} \quad \text{arba} \quad \begin{array}{r} **c\ \ b** \\ \hline **c{+}1\ k** \end{array} \quad \begin{array}{l} \\ a** \end{array};$$

čia $d=a+b$, kai $a+b<10$; $k=a+b-10$, kai $a+b\geqslant 10$.

Ta pati vienėto perkėlimo į aukštesnį skyrių taisyklė teisinga ir bet kuriems sisteminiams skaičiams. Iš tikrųjų, jeigu, pavyzdžiui, $d=a+b<g$, tai

$$(cg^{m+1}+bg^m)+ag^m=cg^{m+1}+dg^m.$$

Tuo atveju, kai $a+b>g$, t. y. $a+b=g+k$,

$$(cg^{m+1}+bg^m)+ag^m=cg^{m+1}+(g+k)\,g^m=(c+1)\,g^{m+1}+kg^m.$$

Jokių esminių naujovių nėra ir kituose aritmetiniuose veiksmuose su sisteminiais skaičiais. Daugindami ir dalydami negalime naudotis įprastine daugybos lentele, nes ji yra „dešimtainė". Greiti skaičiavimai bet kurioje sistemoje atliekami naudojantis atitinkama „sistemine" daugybos lentele. Pateikiame daugybos lentelę šešetainėje skaičiavimo sistemoje:

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	10_6	12_6	14_6
3	3	10_6	13_6	20_6	23_6
4	4	12_6	20_6	24_6	32_6
5	5	14_6	23_6	32_6	41_6

3 *teoremoje pateiktą skaičiaus a* (1.10) *išraišką, kurią sutrumpintai žymėsime*

$$a=\overline{b_k b_{k-1}\ldots b_1 b_0}_{(g)},$$

vadiname to skaičiaus užrašu (išraiška) skaičiavimo sistemoje pagrindu g (g-ainėje skaičiavimo sistemoje). Koeficientai b_i, esantys toje išraiškoje, vadinami *skaičiaus a skaitmenimis skaičiavimo sistemoje pagrindu g (g-ainiai skaitmenys).* Jie neneigiami ir ne didesni už $g-1$. Juos lengva gauti dalybos su liekana būdu. Iš tikrųjų, užrašę (1.11) lygybę ir atitinkamai kitas lygybes, gausime:

$$\begin{aligned} a&=gq+b_0,\\ q&=gq_1+b_1,\\ q_1&=gq_2+b_2,\\ &\cdots\cdots\cdots\cdots\\ q_{k-3}&=gq_{k-2}+b_{k-2},\\ q_{k-2}&=gq_{k-1}+b_{k-1}. \end{aligned}$$

Kadangi natūriniai skaičiai q_i nuosekliai mažėja, tai po baigtinio tokių dalybos žingsnių skaičiaus gausime kurį nors eilinį nepilnąjį santykį q_l, sakykime, q_{k-1}, mažesnį už g. Pažymėkime $q_{k-1}=b_k$. Dabar tik lieka surašyti eilės tvarka, kaip skaitmenis sistemoje g, liekanas b_i ir b_k. Taigi

$$
\begin{aligned}
a &= gq + b_0 = \\
&= g(gq_1 + b_1) + b_0 = g^2 q_1 + gb_1 + b_0 = \\
&= g(gq_2 + b_2) + gb_1 + b_0 = g^3 q_2 + g^2 b_2 + gb_1 + b_0 = \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&= b_k g^k + b_{k-1} g^{k-1} + \ldots + gb_1 + b_0 = \\
&= \overline{b_k b_{k-1} \ldots b_2 b_1 b_{0(g)}}.
\end{aligned}
$$

Pavyzdys. Atliksime keletą veiksmų su sisteminiais skaičiais 114_6 ir 25_6:

$$
\begin{array}{llll}
\begin{array}{r} 114_6 \\ +\ 25_6 \\ \hline 143_6 \end{array} &
\begin{array}{r} 114_6 \\ \times\ 25_6 \\ \hline 1022 \\ +\ 232 \\ \hline 3342_6 \end{array} &
\begin{array}{r} 212_6 \\ -\ 114_6 \\ \hline 54_6 \end{array} &
\begin{array}{r|l} 3342_6 & 35_6 \\ -\ 311 & \overline{54_6} \\ \hline -\ 232 & \\ \hline 232 & \\ -\ 232 & \\ \hline 0 & \end{array}
\end{array}
$$

Paaiškinsime skaičiaus 114_6 daugybą iš 5. Dauginame įprasta tvarka – iš dešinės. Šešetainėje daugybos lentelėje randame $5\times4=32_6$. Rašome 2, o 3 – „mintyje". Toliau $5\times1=5$ ir dar reikia pridėti 3 perkeltus vienetus. Kadangi $5+3=8=1\cdot6+2=12_6$, tai rašome 2, mintyje – vienetas. Paskutinis etapas – $5\times1=5$ ir dar vienetas – $6=10_6$. Tuo būdu gauname

$$114_6 \cdot 5 = 1022_6.$$

Panašiai atlikti ir kiti skaičiavimai.

Sisteminiams skaičiams nėra teisingi įvairūs dalumo požymiai, kurie remiasi dešimtainių skaičių savybėmis. Pavyzdžiui, šešetainėje skaičiavimo sistemoje 100_6 nesidalija iš 5, skaičius 12_7 nėra lyginis, o 13_6 – pirminis. Tuo tarpu 21_6 – pirminis skaičius, o 41_6 – pilnasis kvadratas.

§6. Sistemos pagrindo keitimas

Skaičiuojant su sisteminiais skaičiais, reikia mokėti pereiti nuo vieno sistemos pagrindo prie kito. Nurodysime du paprastus sistemos pagrindo keitimo būdus – *daugybos ir dalybos.*

Taikant daugybos būdą, sisteminio skaičiaus užrašas pertvarkomas į tokį reiškinį, kuriame nuosekliai keičiasi daugybos iš sistemos pagrindo ir sudėties veiksmai. Pavyzdžiui, pertvarkysime penkiaženklį sisteminį skaičių:

$$
\begin{aligned}
b &= \overline{a_4 a_3 a_2 a_1 a_{0(g)}} = a_4 g^4 + a_3 g^3 + a_2 g^2 + a_1 g + a_0 = \\
&= (a_4 g^3 + a_3 g^2 + a_2 g + a_1) g + a_0 = \big((a_4 g^2 + a_3 g + a_2) g + a_1\big) g + a_0 = \\
&= \Big(\big((a_4 g + a_3) g + a_2\big) g + a_1\Big) g + a_0.
\end{aligned}
$$

Daugybos būdas. *Norėdami sisteminį skaičių* $\alpha = a_k a_{k-1} \ldots a_2 a_1 a_{0(g)}$ *užrašyti sistemoje nauju pagrindu h, vyriausiąjį skaičiaus* α *koeficientą (pirmąjį iš kairės skaitmenį* a_k*) dauginame iš seno pagrindo g, prie gautos sandaugos pridedame skaitmenį* a_{k-1} *ir gautą sumą vėl dauginame iš g. Prie gautos sandaugos pridedame tolesnį skaitmenį* a_{k-2} *ir sumą vėl dauginame iš g ir t. t. Procesą baigiame pridėję paskutinį skaitmenį* a_0*. Visus skaičiavimus atliekame sistemoje pagrindu h ir gauname skaičiaus* α *išraišką sistemoje pagrindu h.*

Išnagrinėkime pavyzdį. Užrašysime skaičių 317_8 devynetainėje sistemoje. Atliekame šitokią veiksmų naujoje sistemoje seką:

$$3 \times 8 = 24 = 26_9, \quad 26_9 + 1 = 27_9,$$

$$27_9 \times 8 = (2 \cdot 9 + 7)\, 8 = 16 \cdot 9 + 56 = 16 \cdot 9 + 6 \cdot 9 + 2 =$$

$$= 22 \cdot 9 + 2 = (2 \cdot 9 + 4)\, 9 + 2 = 2 \cdot 9^2 + 4 \cdot 9 + 2 = 242_9.$$

$$242_9 + 7 = 250_9.$$

Taigi $317_8 = 250_9$.

Devynetainėje sistemoje užrašytą skaičių 250_9 „grąžinsime“ į aštuonetainę sistemą. Kadangi dabar skaičiavimus reikia atlikti aštuonetainėje sistemoje, tai vietoje 9 turime rašyti jo išraišką aštuonetainėje sistemoje: $9 = 11_8$. Gausime

$$2 \times 9 = 2 \times 11_8 = 22_8, \quad 22_8 + 5 = 27_8,$$

$$27_8 \times 9 = 27_8 \times 11_8.$$

Skaičiuodami sandaugą $27_9 \times 8$, faktiškai rėmėmės dešimtaine daugybos lentele ir tik skaičiavimo pabaigoje parašėme rezultatą — skaičių 242_9 devynetainėje sistemoje. Tačiau galime dauginti ir įprastu būdu. Tuomet sandaugą $27_8 \times 11_8$ rasime šitaip:

$$\begin{array}{r} \times\ 27_8 \\ \hline 11_8 \\ \hline + \quad 27_8 \\ 27_8 \\ \hline 317_8 \end{array}$$

Paskutinis skaičiavimo etapas, nurodytas taisyklėje, šio rezultato nekeičia:

$$317_8 + 0 = 317_8.$$

Antroji perėjimo nuo vieno sistemos pagrindo prie kito taisyklė paremta dalybos su liekana teorema.

Iš (1.10) arba (1.11) išplaukia, kad natūrinio skaičiaus a, užrašyto sistemoje pagrindu g, paskutinis skaitmuo b_0 yra skaičiaus a dalybos iš g liekana. Tos dalybos veiksmo (nepilnasis) santykis yra

$$q = b_k g^{k-1} + \ldots + b_2 g + b_1.$$

Dalydami q iš g, gauname liekaną b_1, kuri yra skaičiaus a antrasis iš dešinės skaitmuo sistemoje pagrindu g. Tęsdami toliau tą procesą, randame visus skaičiaus a skaitmenis sistemoje pagrindu g. Norėdami rasti a skaitmenis sistemoje pagrindu h, atitinkamai turime dalyti iš h. Taigi teisinga šitokia taisyklė.

Dalybos būdas. *Norėdami skaičių α užrašyti sistemoje pagrindu h, turime α ir visus toliau gaunamus nepilnuosius santykius nuosekliai dalyti iš h su liekana. Procesą baigiame, kai nepilnąjį santykį gauname mažesnį už h. Visos gautosios liekanos bus lygios skaičiaus α skaitmenims (skaitant iš dešinės į kairę) sistemoje h.*

Pavyzdys. Užrašysime skaičių 317_8 devynetainėje sistemoje dalybos būdu. Dalijame iš $h=9=11_8$:

$$\begin{array}{r|l} -\,317_8 & 11_8 \\ \underline{22} & \\ -\,77 & -\,27_8 \;\; \underline{|\; 11_8} \\ \underline{77} & \underline{22} \quad 2 \\ 0 & 5 \end{array}$$

Gautosios liekanos 0 ir 5 bei paskutinis santykis 2 yra to skaičiaus skaitmenys devynetainėje sistemoje. Taigi

$$317_8=250_9.$$

Tuo pačiu būdu skaičių 250_9 grąžinsime į aštuonetainę sistemą:

$$\begin{array}{r|l} -\,250_9 & 8 \\ \underline{17} & \\ -\,70 & -\,27_9 \;\; \underline{|\; 8} \\ \underline{62} & \underline{26} \quad 3 \\ 7 & 1 \end{array}$$

Gautosios liekanos 7 ir 1 bei paskutinis santykis 3 ir yra skaitmenys aštuonetainėje sistemoje (skaitant iš dešinės):

$$250_9=317_8.$$

Tarpiniuose skaičiavimuose paprastumo dėlei neprirašinėjome pagrindo, bet jis toks pat visuose to paties pavyzdžio skaičiavimuose.

Beje, dalybos būdas ir yra tas nuoseklus dalybos su liekana teoremos taikymo būdas, minėtas pastabose po 3 teoremos įrodymo.

Dvejetainė ir aštuonetainė skaičiavimo sistemos. Atskirai aptarsime sistemas pagrindu 2 ir 8. Kaip jau minėjome, jos vartojamos šiuolaikinėje skaičiavimo technikoje.

Dvejetainėje sistemoje yra tik du skaitmenys – 0 ir 1. Bet kuris skaičius, užrašytas toje sistemoje, išreiškiamas tam tikra vienetų ir nulių seka. Pavyzdžiui,

$$2=10_2,\quad 3=11_2,\quad 4=100_2,\quad 5=101_2.$$

Šioje sistemoje palyginti nesunku atlikti sudėties ir daugybos veiksmus. Daugybos lentelė triviali.

Sudauginsime, pavyzdžiui, skaičius 1011_2 ir 101_2:

$$\begin{array}{r} \times\begin{array}{r}1011_2\\ 101_2\end{array} \\ \hline +\begin{array}{r}1011\\ 1011\end{array} \\ \hline 110111_2 \end{array}$$

Vienintelis dalykas, kuo ši daugyba skiriasi nuo atitinkamų dešimtainių skaičių daugybos – reikia atsiminti, kad $1+1=10_2$. Ir dvejetainei, ir aštuonetainei sistemai teisingi visi tie teiginiai, kurie buvo minėti kalbant apie skaičiavimo sistemas praeitame paragrafe. Tačiau šiuo atveju taisyklės, rodančios, kaip pereiti nuo dvejetainės sistemos prie aštuonetainės ir atvirkščiai, yra paprastesnės.

I taisyklė. *Norint dvejetainės sistemos skaičių α užrašyti aštuonetainėje sistemoje, reikia α skaitmenis suskirstyti iš dešinės į kairę grupėmis po 3 skaitmenis (paskutinė – kairioji grupė gali būti nepilna). Gautuosius triženklius dvejetainius skaičius kiekvieną atskirai reikia išreikšti aštuonetainės sistemos skaičiumi – jie bus skaičiaus α skaitmenys aštuonetainėje sistemoje.*

Taisyklė paremta sistemos pagrindo keitimu dalybos būdu, išnagrinėtu praeitame paragrafe. Jeigu

$$\alpha=\overline{a_k a_{k-1}\ldots a_3 a_2 a_1 a_{0(2)}},$$

tai, dalydami jį iš $8=1000_2$, gauname nepilnąjį santykį

$$q=\overline{a_k\ldots a_{3(2)}}$$

ir liekaną

$$\overline{a_2 a_1 a_{0(2)}}=a_2\cdot 2^2+a_1\cdot 2+a_0.$$

Kadangi dvejetainėje sistemoje visi skaitmenys $a_i\leqslant 1$, tai ši liekana

$$a_2\cdot 2^2+a_1\cdot 2+a_0\leqslant 2^2+2+1=7$$

ir yra vienaženklis skaičius aštuonetainėje sistemoje – skaičiaus α skaitmuo toje sistemoje. Taigi radome paskutinį skaičiaus α skaitmenį aštuonetainėje sistemoje – skaičių

$$\overline{a_2 a_1 a_{0(2)}}.$$

Taikydami toliau tą algoritmą su nepilnuoju santykiu

$$q=\overline{a_k a_{k-1}\ldots a_6 a_5 a_4 a_{3(2)}},$$

gauname antrąjį skaičiaus α skaitmenį (iš dešinės) aštuonetainėje sistemoje

$$\overline{a_5 a_4 a_{3(2)}}$$

ir t. t. Taip ir įsitikiname, kad taisyklė teisinga.

Pavyzdys. Dvejetainėje sistemoje užrašytą skaičių

$$1001|101|101010_2$$

suskirstome iš dešinės į grupes po 3 skaitmenis:

$$10\,|\,011\,|\,011\,|\,101\,|\,010_2.$$

Kadangi $10_2=2$, $011_2=3$, $101_2=5$, $010_2=2$, tai

$$1001|101|101|010_2=23352_8.$$

II taisyklė. *Norint aštuonetainės sistemos skaičių α užrašyti dvejetainėje sistemoje, reikia kiekvieną jo skaitmenį užrašyti triženkliu dvejetainės sistemos skaičiumi (prirašant, jei reikia, pradžioje nulius) ir gautuosius skaičius parašyti kaip vieną skaičių, nekeičiant jų tvarkos.*

Taisyklė išplaukia iš I taisyklės ir skaičiaus išraiškos bet kurioje sistemoje vienaties.

Pavyzdys. Užrašysime skaičių 31702_8 dvejetainėje sistemoje. Kadangi $3=11_2$, $1=001_2$, $7=111_2$, $0=000_2$, $2=010_2$, tai

$$31702_8=11001111000010_2.$$

Dvejetainė skaičiavimo sistema patogesnė ir ekonomiškesnė už visas kitas. Jeigu, pavyzdžiui, kiekvienam dešimtainės sistemos triženkliam skaičiui mašinoje reikėtų skirti 30 skirsnių (3 skaitmenys, iš kurių kiekvienas gali įgyti 10 reikšmių), tai tam pačiam skaičiui, užrašytam dvejetainėje sistemoje, reikia tik 20 skirsnių (ne daugiau kaip 10 skaitmenų, iš kurių kiekvienas gali įgyti 2 reikšmes). Įrodyta, kad ekonomiškiausia būtų skaičiavimo sistema pagrindu $e=2{,}718\ldots$, taigi artimiausia jai skaičiavimo sistema sveikuoju pagrindu būtų trejetainė.

Dar kelios pastabos apie sisteminius skaičius.

Bet kuriuos veiksmus su sisteminiais skaičiais galima atlikti tik užrašius juos sistemoje tuo pačiu pagrindu.

Jeigu sistemos pagrindas $g>10$, tai dviženkliai dešimtainiai skaičiai n, $10\leqslant n<g$, toje sistemoje yra vienaženkliai, jų žymėjimui tenka įvesti specialius skaitmenis. Pavyzdžiui, tryliktainė sistema turės 13 skaitmenų:

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ \underbrace{(10)},\ \underbrace{(11)},\ \underbrace{(12)}$$

(neieškant paskutiniams trims skaičiams specialaus ženklo, jie apvesti rutuliukais). Skaičiavimai su tokiais skaitmenimis atliekami įprasta tvarka. Pavyzdžiui,

$$\begin{array}{r} 4\,\underbrace{(10)}\quad 1\,\underbrace{(12)}_{13} \\ +\quad \underbrace{(11)}\,\underbrace{(11)}\quad 2_{13} \\ \hline 5\quad 9\quad 0\quad 1_{13} \end{array} \qquad \begin{array}{r} \underbrace{(12)}\,5\quad 5\,\underbrace{(11)}_{13} \\ +\quad 8\,\underbrace{(10)}\quad 1_{13} \\ \hline 1\quad 0\quad 1\quad 2\,\underbrace{(12)}_{13} \end{array} \qquad \begin{array}{r} 1\quad 9\quad 7\quad 2_{13} \\ \times \qquad\qquad 6_{13} \\ \hline \underbrace{(10)}\,5\quad 3\,\underbrace{(12)}_{13} \end{array}$$

Tai, kas išdėstyta apie sisteminius skaičius, tinka ir dešimtainėje skaičiavimo sistemoje užrašytiems skaičiams.

27. Sudarykite vienaženklių skaičių daugybos lenteles skaičiavimo sistemose pagrindu g, kai:

a) $g=7$; b) $g=8$; c) $g=9$; d) $g=11$; e) $g=12$.

28. Užrašykite skaičius 12, 18, 25, 32, 41, 59, 64, 100, 120, 124 dvejetainėje skaičiavimo sistemoje.

29. Užrašykite dvejetainės skaičiavimo sistemos skaičius 11, 101, 1101, 10011, 111111, 1011011, 111000111, 1101101100 aštuonetainėje sistemoje.

30. Užrašykite dvejetainės skaičiavimo sistemos skaičius 11, 110, 111, 1011, 1101, 11011, 10111, 101110, 110110, 1110111, 1101100, 1111111 dešimtainėje sistemoje.

31. Atlikite aritmetinius veiksmus: 4151_6+525_6, 377_9-288_9, $515_7 \cdot 635_7$, $264_8 : 55_8$.

32. Užrašykite skaičius 4010, 312_4, 8818_9, 157_8, 366_7, 431_5, 212_3, 111_2 šešetainėje skaičiavimo sistemoje abiem (daugybos ir dalybos) būdais.

33. Užrašykite skaičius 421, 181_9, 7719_{12}, 997_{11}, 371_8, 141_7, 225_6, 1101_2 tryliktainėje skaičiavimo sistemoje.

34. Atlikite veiksmus: 315_8-315_7, $519+451_8$, $327_8 \cdot 1101_2$, $101_2\,101_2$.

35. Nustatykite, kurioje skaičiavimo sistemoje $g \leqslant 11$ užrašytas skaičius 1441, jeigu jį dalydami iš 7 gauname liekaną 1.

36. Raskite tokį triženklį dešimtainės sistemos skaičių x, kuris užrašytas tais pačiais skaitmenimis ir ta pačia tvarka, tik kitoje skaičiavimo sistemoje jis 2 kartus didesnis už x.

37. Raskite 3 skaitmenis turintį septynetainės sistemos skaičių, kuris devynetainėje sistemoje užrašomas tais pačiais skaitmenimis, tik atvirkščia tvarka.

§7. Didžiausias bendrasis daliklis ir mažiausias bendrasis kartotinis

Didžiausias bendrasis daliklis. Sveikojo skaičiaus a natūrinių daliklių aibę žymėsime D_a. Dviejų skaičių a ir b daliklių aibių D_a ir D_b sankirta yra jų bendrųjų daliklių (iš kurių dalijasi ir skaičius a, ir skaičius b) aibė. Analogiškai skaičių $a_1, a_2, \ldots, a_n$ bendrieji dalikliai yra sankirtos

$$D = D_{a_1} \cap D_{a_2} \cap \ldots \cap D_{a_n}$$

elementai. Aibė D nėra tuščia, nes jai visuomet priklauso skaičius 1. D yra baigtinė aibė, nes jos didžiausias elementas negali būti didesnis už bet kurį iš skaičių $a_1, a_2, \ldots, a_n$. Pagal didžiausiojo skaičiaus principą aibėje D yra didžiausias elementas.

Skaičių $a_1, a_2, \ldots, a_n$ bendrųjų daliklių aibės D *didžiausias elementas vadinamas didžiausiu šių skaičių bendruoju dalikliu (sutrumpintai d. b. d.).*

Skaičių $a_1, a_2, \ldots, a_n$ didžiausias bendrasis daliklis žymimas įvairiai. Vidurinėje mokykloje jam žymėti vartojamas simbolis $D(a_1, a_2, \ldots, a_n)$. Matematinėje literatūroje paprastai raidė D praleidžiama ir didžiausias bendrasis daliklis žymimas

$$(a_1, a_2, \ldots, a_n).$$

Pavyzdys. Skaičių 24, 42, 60 daliklių aibės yra

$D_{24}=\{1, 2, 3, 4, 6, 8, 12, 24\}$,
$D_{42}=\{1, 2, 3, 6, 7, 14, 21, 42\}$,
$D_{60}=\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$,

jų bendrųjų daliklių aibė

$$D=D_{24}\cap D_{42}\cap D_{60}=\{1,\ 2,\ 3,\ 6\}.$$

Didžiausias tų skaičių bendrasis daliklis yra 6:

$$(24,\ 42,\ 60)=6.$$

Matome, kad skaičių 24, 42, 60 d. b. d. dalijasi iš tų skaičių kitų bendrųjų daliklių. Įsitikinsime, kad tai ne atsitiktinis sutapimas, o bendras dėsnis.

Šis dėsnis įrodomas labai paprastai, įvedus ir išnagrinėjus naują – *modulio* – sąvoką. Žodis „modulis" matematikoje turi keletą prasmių. Jau vartojome terminą „skaičiaus modulis" (absoliutinis didumas). Dabar įvesime modulio, kaip tam tikros aibės, sąvoką.

Sveikųjų skaičių aibės poaibis A, pasižymintis savybėmis

$$u,\ v\in A\Rightarrow u-v\in A,$$
$$u\in A\Rightarrow(\forall s\in Z)us\in A, \tag{1.12}$$

vadinamas moduliu.

Pavyzdžiui, visi lyginiai skaičiai sudaro modulį. Jį sudaro ir vienas skaičius 0, tačiau to atvejo nenagrinėsime.

4 teorema. *Modulio skaičiai yra jo mažiausio teigiamo elemento kartotiniai.*

Įrodymas. Jeigu moduliui A priklauso nelygus nuliui skaičius a, tai jam priklauso ir skaičius $0=a-a$, taip pat ir skaičiui a priešingas skaičius $-a=0-a$. Vadinasi, modulyje yra teigiamų skaičių. Mažiausią iš jų žymėsime raide δ. Tarkime, kad a yra bet kuris modulio A elementas, ir padalykime a iš δ su liekana:

$$a=q\delta+r,$$
$$0\leqslant r<\delta.$$

Tačiau

$$a\in A\wedge\delta\in A\Rightarrow a\in A\wedge q\delta\in A\Rightarrow a-q\delta=r\in A.$$

Kadangi δ yra mažiausias modulio A teigiamas elementas, o $r<\delta$, tai r negali būti teigiamas. Vadinasi, $r=0$.

5 teorema. *Egzistuoja tokie sveikieji skaičiai $x_1, x_2, \ldots, x_n$, kad skaičių $a_1, a_2, \ldots, a_n$ didžiausią bendrąjį daliklį d galima išreikšti šitaip:*

$$d=a_1x_1+a_2x_2+\ldots+a_nx_n. \tag{1.13}$$

Įrodymas. Raide A žymėsime aibę skaičių, išreiškiamų suma

$$a_1y_1+a_2y_2+\ldots+a_ny_n,$$

kurioje $a_1, a_2, \ldots, a_n$ – teoremos formuluotėje minimi skaičiai, $y_1, y_2, \ldots, y_n$ – bet kurie sveikieji skaičiai. Nesunku patikrinti, ar aibė A yra modulis. Iš tikrųjų, jeigu

$$u = a_1 y_1 + a_2 y_2 + \ldots + a_n y_n \in A,$$

$$v = a_1 y_1' + a_2 y_2' + \ldots + a_n y_n' \in A,$$

tai

$$u - v = a_1 (y_1 - y_1') + a_2 (y_2 - y_2') + \ldots + a_n (y_n - y_n');$$

čia visi skirtumai $y - y'$ yra sveikieji skaičiai, todėl $u - v \in A$. Dar paprasčiau tikrinama antroji modulio sąlyga.

Pagal 4 teoremą visi aibės A elementai dalijasi iš mažiausio teigiamo modulio elemento δ.

Nesunkiai įsitikiname, kad skaičiai $a_1, a_2, \ldots, a_n$ taip pat priklauso moduliui A. Pavyzdžiui, a_1 galima užrašyti šitaip:

$$a_1 = a_1 \cdot 1 + a_2 \cdot 0 + \ldots + a_n \cdot 0$$

ir t. t. Todėl visi skaičiai $a_1, a_2, \ldots, a_n$ taip pat dalijasi iš δ. Vadinasi, δ yra tų skaičių bendrasis daliklis. Skaičių δ, kaip aibės A elementą, taip pat galima išreikšti sandaugų suma:

$$\delta = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n.$$

Raide d pažymėjome skaičių $a_1, a_2, \ldots, a_n$ d. b. d., todėl

$$d = (a_1, a_2, \ldots, a_n) \Rightarrow d \mid a_1 \wedge d \mid a_2 \wedge \ldots \wedge d \mid a_n.$$

Iš čia išplaukia, kad

$$d \mid a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = \delta.$$

Vadinasi, $d \leqslant \delta$. Tačiau δ yra skaičių $a_1, a_2, \ldots, a_n$ bendrasis daliklis, todėl jis ne didesnis už tų skaičių didžiausią bendrąjį daliklį: $\delta \leqslant d$. Iš dviejų pastarųjų nelygybių išplaukia $d = \delta$. Teorema įrodyta.

Iš 5 teoremos išplaukia šios išvados.

1 išvada. *Kelių skaičių didžiausias bendrasis daliklis dalijasi iš kiekvieno jų bendrojo daliklio.*

Įrodymas. Įsitikinome, jog egzistuoja tokie sveikieji skaičiai x_i, kad

$$d = (a_1, a_2, \ldots, a_n) = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n.$$

Jeigu t yra skaičių $a_1, a_2, \ldots, a_n$ bet kuris kitas bendrasis daliklis, tai

$$t \mid a_1 \wedge t \mid a_2 \wedge \ldots \wedge t \mid a_n \Rightarrow t \mid (a_1 x_1 + a_2 x_2 + \ldots + a_n x_n) \Rightarrow t \mid d.$$

2 išvada. *Būtina ir pakankama sąlyga, kad lygtis*

$$a_1 y_1 + a_2 y_2 + \ldots + a_n y_n = b \tag{1.14}$$

su sveikaisiais koeficientais turėtų sveikuosius sprendinius, yra

$$d = (a_1, a_2, \ldots, a_n) \mid b.$$

Įrodymas. Sąlygos būtinumas akivaizdus, nes iš d dalijasi (1.14) lygties kairioji pusė. Vadinasi, dalijasi ir jos dešinioji pusė – skaičius b.

Įrodysime sąlygos pakankamumą. Tarkime, kad $d \mid b$, tada $b=dk$. Pagal 5 teoremą egzistuoja tokie sveikieji skaičiai x_i, kad

$$d=a_1x_1+a_2x_2+\ldots+a_nx_n.$$

Tuomet

$$b=dk=a_1(x_1k)+a_2(x_2k)+\ldots+a_n(x_nk).$$

Tai reiškia, kad lygtis (1.14) turi sveikąjį sprendinį

$$y_i=x_ik, \quad i=1, 2, \ldots, n.$$

Išraišką

$$d=a_1x_1+a_2x_2+\ldots+a_nx_n$$

su sveikaisiais skaičiais x_i vadiname skaičių $a_1, a_2, \ldots, a_n$ didžiausio bendrojo daliklio *tiesine išraiška*. Koeficientai x_i randami nevienareikšmiškai.

Pavyzdžiui, jeigu skaičių 15 ir 20 didžiausio bendrojo daliklio $d=5$ viena iš jo tiesinių išraiškų yra

$$d=15x_0+20y_0,$$

tai kitos skaičiaus $d=5$ tiesinės išraiškos

$$d=15x+20y$$

randamos iš lygybių

$$x=x_0+4t, \quad y=y_0-3t;$$

čia t – bet kuris sveikasis skaičius. Imdami $x_0=-1$, $y_0=1$, o t lygų skaičiams -1, 0, 1, 2, gauname šitokias tiesines d išraiškas:

$$\begin{aligned}5&=15(-5)+20\cdot 4\\&=15(-1)+20\cdot 1\\&=15\cdot 3+20(-2)\\&=15\cdot 7+20(-5).\end{aligned}$$

Ieškant dviejų skaičių a ir b didžiausio bendrojo daliklio tiesinės išraiškos, labai praverčia Euklido algoritmas.

Paminėsime keletą akivaizdžių didžiausio bendrojo daliklio savybių.

1. $(ab, a)=a$, (1.15)
2. $(a, 1)=1$, (1.16)
3. $(0, a)=a$, (1.17)
4. $a=qb+r \Rightarrow (a, b)=(b, r)$. (1.18)

Įrodysime tik paskutinę savybę.

Jeigu δ yra skaičių a, b bendrasis daliklis, tai iš jo dalijasi ir skaičius $a-qb=r$. Ir priešingai, iš bet kurio skaičių b ir r bendrojo daliklio dalijasi

skaičius $qb+r$, t. y. dalijasi a. Skaičių b ir r bendrųjų daliklių aibė sutampa su skaičių a ir b bendrųjų daliklių aibe, taigi sutampa ir tų skaičių porų didžiausi bendrieji dalikliai.

6 teorema. *Dviejų natūrinių skaičių a ir b didžiausias bendrasis daliklis lygus paskutinei nelygiai nuliui liekanai, gautai taikant Euklido algoritmą skaičiams a ir b.*

Įrodymas. Nuosekliai taikome kiekvienai (1.7) algoritmo lygybei 4 d.b.d. savybę:

$$(a, b)=(b, r),$$
$$(b, r)=(r, r_1),$$
$$(r, r_1)=(r_1, r_2),$$
$$\cdots\cdots\cdots\cdots$$
$$(r_{k-2}, r_{k-1})=(r_{k-1}, r_k).$$

Pagal 1 d.b.d. savybę $(r_{k-1}, r_k)=r_k$. Taigi

$$(a, b)=r_k.$$

Pavyzdys. Rasime (112, 78). Taikome Euklido algoritmą:

$$112=78\cdot 1+34,$$
$$78=34\cdot 2+10,$$
$$34=10\cdot 3+4,$$
$$10=4\cdot 2+2,$$
$$4=2\cdot 2.$$

Kadangi paskutinė nelygi nuliui šio algoritmo liekana yra $r_3=2$, tai

$$(112, 78)=2.$$

Pasinaudoję 5 paragrafo (1.9) formule, pagal kurią skaičiams a ir b pritaikyto algoritmo liekaną r_s galima išreikšti skaičiais a ir b, lengvai rasime didžiausio bendrojo daliklio tiesinę išraišką:

$$2=r_3=-a\big((2, 3, 2)\big)+b\big((1, 2, 3, 2)\big);$$

čia $a=112$, $b=78$. Oilerio skliaustams skaičiuoti sudarome lentelę

q_i	1	2	3	2
$((q_1, q_2, \ldots, q_i))$	1	3	10	23
$((q_1, \ldots, q_i))$		2	7	16

Gauname tokią vieną skaičių 112 ir 78 didžiausio bendrojo daliklio išraišką:

$$2=-112\cdot 16+78\cdot 23.$$

Mažiausias bendrasis kartotinis.

Skaičius, kuris dalijasi iš visų skaičių a_1, a_2, ..., a_n, vadinamas tų skaičių bendruoju kartotiniu.

Raide M_a žymėsime skaičiaus a kartotinių aibę. Akivaizdu, kad skaičių a_1, a_2, ..., a_n bendrieji kartotiniai bus aibių

$$M_{a_1},\ M_{a_2},\ \ldots,\ M_{a_n}$$

sankirtos M elementai ir tiktai jie. Pagal mažiausio skaičiaus principą aibėje M egzistuoja mažiausias teigiamas elementas.

Skaičių a_1, a_2, ..., a_n bendrųjų kartotinių aibės M *mažiausias teigiamas elementas vadinamas mažiausiu tų skaičių bendruoju kartotiniu (sutrumpintai m.b.k.).*

Skaičių a_1, a_2, ..., a_n m.b.k. žymimas $[a_1, a_2, \ldots, a_n]$ arba $M[a_1, a_2, \ldots, a_n]$, $K[a_1, a_2, \ldots, a_n]$. Žymėsime pirmuoju būdu.

Matėme, kad kelių skaičių d. b. d. dalijasi iš bet kurio kito tų skaičių bendrojo daliklio. Kelių skaičių m. b. k., kuo netrukus įsitikinsime, pasižymi tam tikra prasme simetriška savybe.

7 teorema. *Kelių skaičių mažiausias bendrasis kartotinis dalija bet kurį kitą tų pačių skaičių bendrąjį kartotinį.*

Įrodymas. Skaičiaus a kartotinių aibė yra modulis. Iš tikrųjų, jeigu m_1 ir m_2 yra du skaičiaus a kartotiniai: $m_1=at_1$, $m_2=at_2$, tai akivaizdu, kad a kartotiniai yra skirtumai $m_1-m_2=a(t_1-t_2)$ ir sandaugos m_iz ($z\in\mathbf{Z}$). Modulio (1.12) sąlygos išpildomos. Todėl ta aibė yra modulis. Analogiškai galime įsitikinti, kad ir kelių skaičių bendrųjų kartotinių aibė M yra modulis. Pagal 4 teoremą visi modulio elementai dalijasi iš mažiausio teigiamo to modulio elemento m, kuris ir yra tų skaičių m. b. k. Teorema įrodyta.

Pavyzdys. Rasime skaičių 8, 12 m. b. k. Skaičiaus 8 kartotiniai yra:

$$-16,\ -8,\ 0,\ 8,\ 16,\ 24.\ 32,\ 40,\ 48,\ 56,\ 64,\ 72,\ \ldots$$

Skaičiaus 12 kartotiniai –

$$-24,\ -12,\ 0,\ 12,\ 24,\ 36,\ 48,\ 60,\ 72,\ \ldots$$

Matome, kad teigiami bendrieji šių skaičių kartotiniai yra

$$24,\ 48,\ 72,\ \ldots$$

Taigi

$$[8,\ 12]=24.$$

Kelių skaičių d. b. d. galima rasti remiantis šitokia rekurentine formule:

$$(a_1, a_2, \ldots, a_n) = \big((a_1, a_2, \ldots, a_{n-1}), a_n\big). \tag{1.19}$$

Iš tikrųjų dviejų skaičių $(a_1, a_2, \ldots, a_{n-1})$, a_n bendrieji dalikliai yra tie patys kaip ir n skaičių $a_1, a_2, \ldots, a_n$. Todėl ir jų didžiausi bendrieji dalikliai yra tie patys.

Analogiškai kelių skaičių m. b. k. galima rasti iš formulės

$$[a_1, a_2, \ldots, a_n] = \big[[a_1, a_2, \ldots, a_{n-1}], a_n\big]. \tag{1.20}$$

Šiuo atveju pakanka įsitikinti, kad sutampa skaičių $a_1, a_2, \ldots, a_n$ bei $[a_1, a_2, \ldots, a_{n-1}]$, a_n bendrųjų kartotinių aibės.

Uždaviniai

38. Įrodykite (1.19) formulę.
39. Įrodykite (1.20) formulę.
40. Įrodykite, kad visi sveikieji skaičiai, kurie dalijasi iš 7, sudaro modulį.
41. Nustatykite, ar sudaro modulį nelyginiai sveikieji skaičiai.
42. Įrodykite, kad sveikieji skaičiai, kurių paskutinis skaitmuo yra 0, sudaro modulį.
43. Raskite skaičių 96, 128, 160 bendruosius daliklius.
44. Parašykite skaičių 24 ir 96 d. b. d. tiesinę išraišką.
45. Raskite (420, 126, 520, 1020, 6000) ir [16, 24, 30, 42].
46. Taikydami Euklido algoritmą, raskite (462, 546), (420, 525), (1058, 1541), (2822, 4641), (840, 252, 1050).
47. Nustatykite, ar lygtys

$$45x+18y+3z=64,\ 13x+12y+11z=10$$

turi sveikųjų sprendinių.
48. Įrodykite lygybę $[ak, bk]=k\,[a, b]$.
49. Įrodykite: jeigu $(a, b)=1$, tai

$$\frac{1}{a}+\frac{1}{a+b}$$

yra nesuprastinama trupmena.

§8. Tarpusavyje pirminiai skaičiai

Akivaizdu, kad bet kurie du gretimi sveikieji skaičiai s ir $s+1$ neturi jokių kitų natūrinių bendrųjų daliklių, išskyrus 1. Tokie skaičiai, kurių d. b. d. yra 1, labai svarbūs dalumo teorijoje.

Skaičiai $a_1, a_2, \ldots, a_n$ vadinami tarpusavyje (reliatyviai) pirminiais, kai jų didžiausias bendrasis daliklis yra 1.

Pavyzdžiui, tokie yra skaičiai 12, 15, 25.

Skaičiai $a_1, a_2, \ldots, a_n$ vadinami poromis tarpusavyje (reliatyviai) pirminiais, kai bet kurių dviejų skaičių didžiausias bendrasis daliklis yra 1.

Pavyzdžiui, skaičiai 10, 15, 9 yra tarpusavyje pirminiai, nes $(10, 15, 9) = 1$. Tie skaičiai nėra poromis tarpusavyje pirminiai, nes $(10, 15) = 5$. Skaičiai 10, 9, 11 poromis tarpusavyje pirminiai, nes $(10, 9) = (10, 11) = (9, 11) = 1$.

Jeigu skaičiai yra poromis tarpusavyje pirminiai, tai jie būtinai ir tarpusavyje pirminiai. Atvirkščias teiginys, kaip matėme pavyzdyje, ne visuomet teisingas. Jeigu turime tik du skaičius, tai abi tos sąvokos sutampa.

Įrodysime kelias teoremas apie tarpusavyje pirminius skaičius.

8 teorema. *Skaičiai a ir b yra tarpusavyje pirminiai tada ir tik tada, kai egzistuoja tokie sveikieji skaičiai x ir y, su kuriais teisinga lygybė*

$$ax + by = 1.$$

Įrodymas. Sąlygos būtinumas išplaukia iš 5 teoremos. Įrodysime, kad ta sąlyga pakankama.

Jeigu $d \mid a$ ir $d \mid b$, tai $d \mid (ax+by)$, t. y. $d \mid 1$. Taigi d gali būti 1.

Išvada. *Jeigu skaičiai a ir b yra tarpusavyje pirminiai, tai tarpusavyje pirminiai yra ir bet kurie jų atitinkami dalikliai a_1 ir b_1.*

Iš tikrųjų, jeigu $a_1 \mid a$ ir $b_1 \mid b$, tai yra tokie sveikieji skaičiai a_2 ir b_2, kad $a = a_1 a_2$, $b = b_1 b_2$. Kadangi skaičiai a ir b tarpusavyje pirminiai, tai yra tokie x ir y, su kuriais

$$ax + by = 1,$$

arba

$$a_1 a_2 x + b_1 b_2 y = 1.$$

Pažymėję $a_2 x = x_1$, $b_2 y = y_1$, turime

$$a_1 x_1 + b_1 y_1 = 1.$$

Iš 8 teoremos išplaukia, kad a_1 ir b_1 yra tarpusavyje pirminiai skaičiai.

9 teorema. *Skaičius a ir b padaliję iš jų d. b. d., gauname tarpusavyje pirminius skaičius.*

Įrodymas. Remiantis 5 teorema,

$$d = ax + by;$$

čia $d = (a, b)$. Padaliję šios lygybės narius iš d, gauname

$$1 = \frac{a}{d} x + \frac{b}{d} y.$$

Toliau telieka remtis 8 teorema.

10 teorema. *Jeigu skaičių a ir b sandauga ab dalijasi iš c ir skaičiai a ir c tarpusavyje pirminiai, tai b dalijasi iš c.*

Įrodymas. Remdamiesi 8 teorema, galime rasti tokius skaičius x ir y, su kuriais

$$ax+cy=1.$$

Padauginę šią lygybę iš b, gauname

$$abx+cby=b.$$

Pagal teoremos sąlygą sandauga ab dalijasi iš c. Sandauga cby, aišku, taip pat dalijasi iš c. Taigi iš c dalijasi kairioji tos lygybės pusė (6 dalumo savybė, § 2). Tačiau tada iš c dalijasi ir dešinioji lygybės pusė – skaičius b.

11 teorema. *Jeigu skaičiai a ir c yra tarpusavyje pirminiai, tai*

$$(a,\ bc)=(a,\ b). \tag{1.21}$$

Įrodymas. Pažymėsime $(a,\ bc)=\delta$ ir $(a,\ b)=d$. Akivaizdu, kad d yra ne tik skaičių a ir b, bet ir skaičių a ir bc bendrasis daliklis. Todėl $d \mid \delta$. Kadangi $(a,\ c)=1$, tai, remdamiesi 8 teorema, galime rasti sveikuosius skaičius x ir y, su kuriais

$$ax+cy=1,$$

arba

$$abx+cby=b.$$

Kadangi iš $\delta=(a,\ bc)$ dalijasi a ir bc, tai iš jo dalijasi ir kairioji paskutinės lygybės pusė. Vadinasi, iš δ dalijasi b. Tačiau iš skaičiaus δ, kuris yra skaičių a ir b bendrasis daliklis, dalijasi ir tų skaičių d. b. d. – skaičius d. Taigi $\delta \mid d$. Iš sąryšių $d \mid \delta$ ir $\delta \mid d$ išplaukia $\delta=d$.

1 išvada. *Jeigu skaičius a yra tarpusavyje pirminis su skaičiais b ir c, tai a tarpusavyje pirminis ir su jų sandauga bc.*

2 išvada. *Jeigu skaičiai a ir b tarpusavyje pirminiai, tai tarpusavyje pirminiai ir bet kurie jų natūriniai laipsniai*:

$$(a,\ b)=1 \Rightarrow (a^n,\ b^m)=1 \quad (n,\ m \in \mathbf{N}).$$

Įrodymas. 11 teoremos (1.21) lygybėje paėmę $b=c$, gauname

$$(a,\ b^2)=(a,\ b)=1.$$

Po to (1.21) lygybėje pakeitę $c=b^2$ ir pasirėmę ką tik užrašyta lygybe, turime

$$(a,\ b^3)=1.$$

Analogiškai samprotaudami, gauname

$$(a,\ b^2)=(a,\ b^3)=\ldots=(a,\ b^n)=1.$$

Kadangi išvados sąlygoje $(a,\ b)=1$ skaičiai a ir b gali būti sukeisti vietomis, tai

$$(a^n,\ b)=1.$$

11 teoremoje skaičių a pakeitę skaičiumi a^n, tokiu pat būdu gausime

$$(a^n, b)=(a^n, b^2)=\ldots=(a^n, b^m)=1.$$

3 išvada. *Jeigu skaičių a ir b natūriniai laipsniai a^n ir b^m tarpusavyje pirminiai, tai ir patys skaičiai a ir b tarpusavyje pirminiai.*

Įrodymas. Jeigu skaičiai a^n ir b^m yra tarpusavyje pirminiai, tai egzistuoja sveikieji skaičiai x ir y, su kuriais

$$a^n x+b^m y=1.$$

Pažymėję $a^{n-1}x=x_1$, $b^{m-1}y=y_1$, tą lygybę galime užrašyti šitaip:

$$ax_1+by_1=1.$$

Toliau reikia remtis 8 teorema.

12 teorema. *Dviejų natūrinių skaičių a ir b didžiausią bendrąjį daliklį ir mažiausią bendrąjį kartotinį sieja lygybė*

$$(a, b)\cdot[a, b]=ab.$$

Įrodymas. Pažymėkime

$$\mathrm{M}=\frac{ab}{(a, b)}.$$

Akivaizdu, kad M yra sveikasis skaičius. Pažymėję $(a, b)=d$, turime

$$a=a_1 d, \quad b=b_1 d.$$

Iš 9 teoremos išplaukia, kad skaičiai a_1 ir b_1 yra tarpusavyje pirminiai. Todėl

$$\mathrm{M}=\frac{a_1 d\cdot b_1 d}{d}=a_1 b_1 d=ab_1=ba_1.$$

Ši lygybė rodo, kad M yra skaičių a ir b kartotinis, taigi jų bendrasis kartotinis. Įrodysime, kad jis yra ir mažiausias bendrasis kartotinis.

Tarkime, kad M_1 yra bet kuris skaičių a ir b bendrasis kartotinis. Taigi egzistuoja tokie sveikieji skaičiai s ir t, kad

$$\mathrm{M}_1=as=bt.$$

Pastarąją lygybę, atsižvelgdami į ankstesnius žymėjimus, galime užrašyti šitaip:

$$a_1 ds=b_1 dt,$$

$$a_1 s=b_1 t.$$

Kadangi, kaip minėjome, skaičiai a_1 ir b_1 yra tarpusavyje pirminiai, tai (10 teorema) skaičius s dalijasi iš b_1:

$$s=b_1 c$$

ir

$$\mathrm{M}_1=a_1 ds=a_1 b_1 dc=\mathrm{M}c.$$

Vadinasi, bet kuris skaičių a ir b kartotinis M_1 dalijasi iš M. Taigi M yra pats mažiausias iš visų a ir b bendrųjų kartotinių, jis yra mažiausias bendrasis kartotinis.

Išvada. *Jeigu skaičiai a ir b tarpusavyje pirminiai, tai jų m.b.k. lygus jų sandaugai.*

Pavyzdžiai. 1. Skaičiai 178 ir 1781 yra tarpusavyje pirminiai, nes $178 \cdot (-10) + 1781 \cdot 1 = 1$.

2. Žinome, kad skaičiai 11 ir 13 yra tarpusavyje pirminiai, todėl galime rasti tokius sveikuosius skaičius x ir y, su kuriais

$$11x + 13y = 1.$$

Galime imti, pavyzdžiui, $x = 6$, $y = -5$.

3. Kadangi, kaip matėme 1 pavyzdyje, skaičiai 178 ir 1781 tarpusavyje pirminiai, tai tokie yra ir skaičiai 178/2 ir 1781/3.

4. Kadangi skaičiai 12 ir 7 tarpusavyje pirminiai, tai

$$(12^7, 7^{13}) = 1.$$

5. Skaičių 18 ir 32 m.b.k. rasime remdamiesi 12 teorema:

$$[18, 32] = \frac{18 \cdot 32}{(18,32)} = \frac{18 \cdot 32}{2} = 288.$$

6. Kadangi $(178, 1781) = 1$, tai

$$[178, 1781] = 178 \cdot 1781 = 317018.$$

Uždaviniai

50. Apibendrinkite 8 teoremą keliems skaičiams.

51. Įrodykite lygybę $(ak, bk) = k(a, b)$.

52. Įrodykite lygybę

$$[a, b, c] = \frac{abc(a, b, c)}{(a, b)(a, c)(b, c)}.$$

53. Įrodykite: jeigu $[a_1, a_2] = m_1$, $[m_1, a_3] = m_2$, ..., $[m_{n-2}, a_n] = m_{n-1}$, tai $[a_1, a_2, \ldots, a_n] = m_{n-1}$.

54. Įrodykite, kad n poromis tarpusavyje pirminių skaičių m. b. k. lygus jų sandaugai.

55. Raskite [2520, 6600], [5640, 2500], [758, 1137].

56. Naudodamiesi 48 uždaviniu, raskite m.b.k. šių skaičių:
a) 232, 460, 280; b) 640, 3200, 4800; c) 24, 36, 48, 64, 96.

57. Įrodykite, kad skaičiai $2n+1$, $9n+4$ ($n \in N$) yra tarpusavyje pirminiai.

58. Įrodykite, kad kiekvienas skaičius $n > 6$ yra suma dviejų tarpusavyje pirminių skaičių, didesnių už 1.

59. Įrodykite, kad lygtis

$$ax + (a+1)y + (a+2)z = a+3$$

visuomet turi sveikąjį sprendinį.

60. Išskaidykite skaičių $3^{10} + 3^5 + 1$.

§9. Neapibrėžtoji lygtis su dviem kintamaisiais

Dviejų kintamųjų su sveikaisiais koeficientais pirmojo laipsnio lygtis

$$ax+by=c \tag{1.22}$$

turi daug realiųjų sprendinių. Todėl ji vadinama *neapibrėžtąja lygtimi*. Siame paragrafe nagrinėsime tik sveikuosius tos lygties sprendinius. Ta papildoma sąlyga, kad sprendiniai turi būti sveikųjų skaičių x, y poros, keičia teiginį apie sprendinių skaičių, keičia ir lygties sprendimo būdą.

Pirmiausia ši lygtis iš viso gali neturėti sprendinių. Taip bus tada, kai skaičius c nesidalys iš koeficientų a ir b didžiausio bendrojo daliklio (5 teoremos 2 išvada). Priešingu atveju, kai c dalijasi iš (a, b), pagal 8 teoremą (1.22) lygtis visuomet išsprendžiama sveikaisiais skaičiais.

Įrodysime, kad tuo atveju sprendinių be galo daug, tačiau jų aibei nustatyti pakanka rasti bent vieną (1.22) lygties sprendinį.

Kadangi ši lygtis išsprendžiama tada ir tik tada, kai c dalijasi iš (a, b), tai visuomet galime lygtį suprastinti visus jos koeficientus padaliję iš skaičių a ir b didžiausio bendrojo daliklio. Todėl laikysime, kad (1.22) lygtyje

$$(a, b)=1.$$

13 teorema. *Jeigu sveikųjų skaičių x_0, y_0 pora yra lygties*

$$ax+by=c, \quad (a, b)=1,$$

sprendinys, tai visi kiti sveikieji tos lygties sprendiniai x, y randami iš lygybių

$$x=x_0+bt,$$

$$y=y_0-at;$$

čia t – bet koks sveikasis skaičius.

Įrodymas. Jeigu, be skaičių x_0, y_0 poros, (1.22) lygties sprendinys yra ir kita pora x_1, y_1, tai

$$ax_0+by_0=c,$$

$$ax_1+by_1=c.$$

Atėmę panariui šias dvi lygybes, gauname

$$a(x_0-x_1)=b(y_1-y_0).$$

Kadangi $(a, b)=1$, tai (10 teorema) iš b dalijasi skirtumas x_0-x_1:

$$x_0-x_1=bt \quad (t\in \mathbf{Z}).$$

Iš šios ir anksčiau užrašytos lygybės randame

$$y_0-y_1=-at.$$

Teorema įrodyta.

Norėdami rasti bent vieną (1.22) lygties sprendinį, galime naudotis Euklido algoritmu.

Įrodinėdami 13 teoremą, laikėme, kad (1.22) lygtis yra suprastinta, t. y. $(a, b)=1$. Gali kilti klausimas, ar nepakeičiame sprendinių aibės dalydami visus lygties $ax+by=c$ narius iš koeficientų a, b, c didžiausio bendrojo daliklio? Tikrai ne. Akivaizdu, kad bet kuris lygties

$$ax+by=c,\ (a,\ b)=1, \tag{1.23}$$

sprendinys x, y yra kartu ir lygties

$$adx+bdy=cd$$

sprendinys, ir atvirkščiai.

Paprasčiausia vietoje (1.23) lygties spręsti pagalbinę lygtį

$$aX+bY=1. \tag{1.24}$$

Jeigu X_0, Y_0 yra kažkuris pastarosios lygties sprendinys, tai skaičių pora X_0c, Y_0c yra (1.23) lygties sprendinys. Radę bent vieną (1.23) lygties sprendinį, kitus jos sprendinius galime rasti naudodamiesi 13 teoremoje pateiktomis formulėmis.

Pavyzdys. Išspręsime lygtį

$$23x-16y=6. \tag{1.25}$$

Jos pagalbinė lygtis yra

$$23X-16Y=1. \tag{1.26}$$

Pagalbinę lygtį galime spręsti naudodamiesi Euklido algoritmu. Atsakymas, kaip lengva įsitikinti, nepriklauso nuo pradinių skaičių ženklų, todėl paprasčiau algoritmą taikyti teigiamų skaičių porai:

$$23=16\cdot 1+7,$$

$$16=7\cdot 2+2,$$

$$7=2\cdot 3+1.$$

Paskutinė (1.7) Euklido algoritmo eilutė čia nereikalinga, nes sprendžiant reikia išreikšti paskutinę nelygią nuliui algoritmo liekaną pradiniais algoritmo skaičiais $|a|$, $|b|$ bei nepilnaisiais santykiais q_i. Šiuo atveju $r_2=1$, $q=1$, $q_1=2$, $q_2=3$. Pasirėmę (1.9) formule, gauname

$$r_2=1=23\cdot\big((2,\ 3)\big)-16\cdot\big((1,\ 2,\ 3)\big).$$

Apskaičiavę Oilerio skliaustus, turime

$$1=23\cdot 7-16\cdot 10.$$

Matome, kad skaičių pora 7, 10 yra (1.26) pagalbinės lygties sprendinys. Beje, jeigu pagalbinėje lygtyje vietoje minuso būtų buvęs pliuso ženklas, tai sprendiniu būtų buvusi pora 7, -10.

Radę vieną pagalbinės lygties sprendinį, galime užrašyti vieną (1.25) lygties sprendinį. Juo bus pora 42, 60. Visi (1.25) lygties sprendiniai pagal 13 teoremą bus

$$x=42+(-16)t=42-16t,$$

$$y=60-23t\ \ (t\in\mathbf{Z}).$$

Trijų kintamųjų lygtis

$$ax+by+cz=d$$

su sveikaisiais koeficientais turi sveikųjų sprendinių tada ir tik tada, kai $(a, b, c) \mid d$. Pažymėję $k=(a, b)$, anksčiau aptartu būdu galime išspręsti lygtį

$$ax+by=k.$$

Tarkime, kad sveikųjų skaičių pora x_0, y_0 yra tos lygties sprendinys:

$$ax_0+by_0=k.$$

Toliau sprendžiame lygtį

$$ku+cz=d.$$

Ši lygtis išsprendžiama, nes

$$(k, c)=\big((a, b), c\big)=(a, b, c),$$

o $(a, b, c) \mid d$. Jeigu u_0, z_0 yra lygties $ku+cz=d$ sprendinys, tai akivaizdu, kad

$$ax_0u_0+by_0u_0+cz_0=d.$$

Vadinasi, sveikųjų skaičių trejetas x_0u_0, y_0u_0, z_0 yra lygties $ax+by+cz=d$ sprendinys.

Lygtys su sveikaisiais koeficientais, kai ieškoma tik sveikųjų sprendinių, vadinamos *Diofanto lygtimis* (III a. Aleksandrijos matematiko Diofanto, nagrinėjusio tokias lygtis, vardu).

Uždaviniai

61. Raskite lygčių $5x+7y=11$, $15x+24y=81$, $73x+94y=1$, $3x+10y+13z=17$, $4x+11y+21z=100$ sveikuosius sprendinius.

62. Raskite lygčių $3x+5y=31$, $8y+13z=58$, $4x^2+x+y=18$, $3x^2+2y^2+7y=21$, $x^3+2x^2+3x+y^4=103$ natūrinius sprendinius.

§10. Pirminiai ir sudėtiniai skaičiai. Eratosteno rėtis

Skaičių teorijoje svarbią vietą užima pirminiai skaičiai. Priminsime jų apibrėžimą.

Natūriniai skaičiai $p>1$, neturintys netrivialiųjų daliklių, vadinami pirminiais.

Pirminius skaičius žymėsime raide p. Iš jų apibrėžimo išplaukia, kad vieninteliai natūriniai pirminio skaičiaus p dalikliai yra 1 ir p.

Skaičius 1 taip pat neturi netrivialiųjų daliklių, tačiau sutarta jo nepriskirti prie pirminių skaičių. Dėl to supaprastėja kai kurių dėsnių formuluotės.

Natūriniai skaičiai $n>1$, turintys netrivialiųjų daliklių, vadinami sudėtiniais skaičiais.

Taigi kiekvienas sudėtinis skaičius turi bent vieną netrivialųjį daliklį. Natūriniai skaičiai skirstomi į 3 kategorijas:

a) skaičius 1,

b) pirminiai skaičiai: 2, 3, 5, 7, 11, 13, ...

c) sudėtiniai skaičiai: 4, 6, 8, 9, 10, 12, ...

Matome, kad yra tik vienas lyginis pirminis skaičius 2, kiti pirminiai skaičiai – nelyginiai.

Pirminių skaičių reikšmė dalumo teorijoje dalinai išryškėja iš šios teoremos.

14 teorema. *Bet kuris skaičius $n>1$ turi pirminį daliklį.*

Įrodymas. Raide M žymėsime aibę skaičiaus n daliklių, didesnių už 1. Pagal mažiausiojo skaičiaus principą aibėje M egzistuoja mažiausias elementas; jį žymėsime p. Skaičius p didesnis už 1, bet jis negali būti sudėtinis, nes iš sąryšių

$$d \mid p \quad (1<d<p) \quad \text{ir} \quad p \mid n$$

išplauktų (žr. 5 dalumo savybę) $d \mid n$ $(1<d<p)$, bet tai prieštarauja prielaidai, kad p yra mažiausias skaičiaus n daliklis, didesnis už 1.

Taigi p yra pirminis skaičius. Teorema įrodyta.

Iš teoremos išplaukia šios išvados.

1 išvada. *Mažiausias natūrinio skaičiaus netrivialusis daliklis yra pirminis skaičius.*

Tuo įsitikinome įrodinėdami teoremą.

2 išvada. *Kiekvienas sudėtinis skaičius n turi daliklį d, tenkinantį nelygybę*

$$1<d\leqslant\sqrt{n}.$$

Įrodymas. Jeigu d yra netrivialusis skaičiaus n daliklis, d' – jo papildomasis daliklis (taip pat netrivialus), tai

$$n=dd'.$$

Akivaizdu, kad abu tie skaičiaus n dalikliai kartu negali būti didesni už $\sqrt{n}$.

3 išvada. *Bet kuris sudėtinis skaičius n turi bent vieną pirminį daliklį $p\leqslant\sqrt{n}$.*

Ta išvada išplaukia iš dviejų pirmųjų.

4 išvada. *Jeigu skaičius* $n>1$ *neturi netrivialiųjų daliklių* d, $d\leqslant\sqrt{n}$, *tai jis yra pirminis.*

Remdamiesi pastarosiomis dviem išvadomis, galime nustatyti, ar skaičius n yra pirminis, ar sudėtinis. Pakanka patikrinti, ar jis turi pirminį daliklį p, ne didesnį už $\sqrt{n}$.

Pavyzdys. Patikrinsime, pirminis ar sudėtinis yra skaičius 103. Pagal 3 išvadą, jeigu skaičius 103 sudėtinis, tai turi būti bent vienas pirminis daliklis $p\leqslant\sqrt{103}$. Tačiau visi pirminiai skaičiai, ne didesni už $\sqrt{103}$, yra 2, 3, 5, 7 ir nė vienas iš jų nedalija 103. Taigi nustatėme, kad skaičius 103 yra pirminis.

Eratosteno rėtis. Jau senovės graikų matematiko *Eratosteno* (276–194 m. pr. m. e.) raštuose randame įdomią idėją, kaip iš natūrinių skaičių aibės galima būtų išskirti pirminius skaičius. Ta idėja pagrįstą metodą, matematikos istorijoje žinomą *Eratosteno rėčio* pavadinimu, nusako ši teorema.

15 (Eratosteno rėčio) teorema. 1. *Jeigu natūrinių skaičių sekoje*

$$2,\ 3,\ 4,\ \ldots,\ N$$

išbrauksime keletą pirmųjų pirminių skaičių ir visus jų kartotinius, tai pirmasis likęs neišbrauktas skaičius bus pirminis.

2. *Jeigu toje pačioje sekoje išbrauksime visus pirminius skaičius, ne didesnius už* $\sqrt{N}$, *ir jų kartotinius, tai visi likusieji skaičiai bus pirminiai ir tenkins sąlygą*

$$\sqrt{N}<p\leqslant N.$$

Įrodymas. 1. Jeigu pirmasis likęs skaičius $a>1$ būtų sudėtinis, tai jis turėtų pirminį daliklį p. Tačiau $p<a$, todėl tas pirminis skaičius buvo išbrauktas. Vadinasi, turėjo būti išbrauktas ir jo kartotinis a. Taigi a nėra sudėtinis.

2. Pirminiai skaičiai, ne didesni už $\sqrt{N}$, išbraukti. Bet kuris sudėtinis skaičius $n\leqslant N$ turi pirminį daliklį, ne didesnį už $\sqrt{N}$, taigi pagal teoremos sąlygą yra išbrauktas.

Teorema įrodyta.

Remdamiesi ta teorema, galime išskirti pirminius skaičius. Sekoje

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ \ldots,\ N$$

pirmasis skaičius 2 yra pirminis. Išbraukiame jį ir visus jo kartotinius. Pirmasis iš likusių skaičių yra pirminis skaičius 3:

$$3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15,\ \ldots$$

Išbraukiame skaičių 3 ir visus jo kartotinius. Pirmasis iš likusių skaičių yra pirminis 5:

$$5,\ 7,\ 11,\ 13,\ 17,\ 19,\ \ldots$$

Taip braukome toliau, kol išbraukiame visų pirminių skaičių $p \leqslant \sqrt{N}$ kartotinius. Visi likusieji skaičiai yra taip pat pirminiai p, be to,

$$\sqrt{N} < p \leqslant N.$$

Suprantama, kai skaičius N didelis, tas pirminių skaičių išskyrimo būdas ne itin patogus. Didesnius skaičiavimus padeda atlikti elektroninės skaičiavimo mašinos. Su jų pagalba sudaromos didelės pirminių skaičių lentelės. 1959 m. *K. Beikeris* ir *F. Grunbergeris* paruošė mikrofilmą, kuriame surašyti visi pirminiai skaičiai, ne didesni už 104 395 301. Jų yra 6 milijonai.

Eratosteno laikais skaičiai buvo surašomi lentelėse. Atrenkant pirminius skaičius, jų kartotiniai būdavo išduriami. Likdavo skylėta lentelė, primenanti rėtį. Iš čia ir kilęs rėčio pavadinimas.

Šiuolaikinėje matematikoje Eratosteno rėčio idėja remiamasi nagrinėjant pirminių skaičių ir kitas problemas. Ta idėja paremti metodai vadinami *rėčio metodais.*

Pirminiai skaičiai buvo ir yra mėgstamas matematikų tyrimo objektas. Tam tikro pavidalo pirminiai skaičiai įėjo į matematikos istoriją kartu su juos nagrinėjusių matematikų vardais.

XVII a. prancūzų matematikas *Mersenas* (M. Mersenne, 1588–1648) tyrė 2^n-1 pavidalo skaičius. Šio pavidalo pirminiai skaičiai jo garbei buvo pavadinti *Merseno pirminiais skaičiais*. Juos žymėsime M_n.

Jeigu n – sudėtinis skaičius, tai nesunku įsitikinti, kad ir 2^n-1 yra sudėtinis. (Jeigu n – nelyginis, tai 2^n-1 dalijasi iš $2^{n/d}-1$, kai n dalijasi iš d; jeigu n – lyginis, tai 2^n-1 dalijasi iš $2^{n/2}-1$.) Taigi Merseno pirminiai skaičiai turi būti 2^p-1 pavidalo, p – pirminis skaičius. Tačiau ne su visais pirminiais skaičiais p skirtumas 2^p-1 yra pirminis skaičius.

Merseno pirminius skaičius gauname, kai $p=2, 3, 5, 7, 13, 17, 19$, tačiau kai $p=11, 23, 29$, skaičiai 2^p-1 yra sudėtiniai. Jeigu skaičiai p dideli, reikia atlikti daug skaičiavimų, norint nustatyti, koks yra skaičius 2^p-1. Konkretūs skaičiavimai matematikos istorijoje susieti su juos atlikusių mokslininkų vardais.

1750 m. žymusis Peterburgo akademikas *Leonardas Oileris* (L. Euler, 1707–1783) įrodė, kad Merseno skaičius $M_{31}=2^{31}-1$ yra pirminis. 1876 m. *E. Liuka* (E. Lucas) nustatė, kad M_{127} yra pirminis. 1883 m. *I. Pervušinas* įrodė, kad M_{61} yra pirminis. 1907 ir 1914 m. *Pauersas* rado dar du Merseno pirminius skaičius – M_{89} ir M_{107}. 1963 m. didžiausiu Merseno pirminiu skaičiumi buvo laikomas M_{11213}. Ilinojaus universiteto (JAV) elektroninė skaičiavimo mašina skaičiavo 2 valandas ir 15 minučių, kol nustatė, kad tas skaičius yra pirminis...

Pradėjus naudotis kompiuteriais, paspartėjo kai kurių problemų sprendimas, bet prieš labai didelius skaičius ir skaičiavimo technika bejėgė. Pastaruoju metu žinomi 28 Merseno pirminiai skaičiai, didžiausias iš jų – M_{86243}, rastas 1983 m. Tiesa, nežinia, ar jis yra 28-asis iš eilės Merseno skaičius. Taip pat nežinoma, ar Merseno pirminių skaičių aibė yra begalinė.

Nėra patogių kriterijų, kuriais remiantis galima būtų patikrinti, ar skaičius pirminis, ar ne. Paminėsime porą kriterijų, kuriuos dar XVIII a. nustatė Oileris.

Pirmasis Oilerio kriterijus. *Jeigu nelyginis natūrinis skaičius $N>1$ gali būti išreikštas dviejų natūrinių skaičių kvadratų skirtumu daugiau kaip vienu būdu, tai N yra sudėtinis; jeigu tik vienu būdu, tai N yra pirminis.*

Įrodymas. Jeigu N – pirminis ir $N=m^2-n^2=(m-n)(m+n)$, tai turi būti $m-n=1$, $m+n=N$. Tokiu būdu skaičius m ir n randame vienareikšmiškai ir $N=((N+1)/2)^2-((N-1)/2)^2$. Kitokia skaičiaus N išraiška natūrinių skaičių kvadratų skirtumu negalima.

Jeigu N – sudėtinis skaičius, t. y. $N=ab$, $a>b>1$, tai abu skaičiai a ir b yra nelyginiai. Gauname dar vieną skaičiaus N išraišką $N=ab=x^2-y^2$; čia $x=(a+b)/2$, $y=(a-b)/2$.

Antrasis Oilerio kriterijus. *Jeigu natūrinis skaičius N gali būti išreikštas dviejų natūrinių skaičių kvadratų suma daugiau kaip vienu būdu, tai N yra sudėtinis.*

Įrodoma panašiai kaip ir pirmuoju atveju.

Dar P. Ferma įrodė, kad $4t+1$ pavidalo natūrinius skaičius galima užrašyti dviejų kvadratų suma, o $4t+3$ pavidalo skaičių negalima taip užrašyti. Ar daug yra pirminių skaičių, kuriuos galima užrašyti kvadratų suma $p=a^2+b^2$? Taip, be galo daug. Tačiau ar yra be galo daug $p=a^2+1$ pavidalo pirminių skaičių? Ši problema neišspręsta iki šiol. Ji žinoma *Landau hipotezės* vardu. Beje, šią problemą nagrinėjo ir Lietuvos matematikas prof. *J. Kubilius*. Apie tai dar šiek tiek kalbėsime nagrinėdami pirminių skaičių pasiskirstymo klausimus.

Kai kurios pirminių skaičių problemos jau išgvildentos. Galime paminėti garsią istorinę problemą, vadinamą *Bertrano postulatu*: kai $n>7$, tarp skaičių n ir $2n-2$ yra pirminis skaičius. Bertrano postulatą 1852 m. įrodė rusų matematikas *P. Čebyšovas*.

Kaip savotiška šio postulato priešingybė (aišku, jo nepaneigianti) yra tvirtinimas, kad galima rasti kiek norima ilgą intervalą, kuriame nėra nė vieno pirminio skaičiaus. Pavyzdžiui, milijono natūrinių skaičių ilgumo intervalas, kuriame nėra pirminių, prasideda skaičiumi $(10^6+1)!+2$. Kad toks intervalas iš tikrųjų yra, paliekame įsitikinti skaitytojui.

Baigdami šį paragrafą, atkreipsime dėmesį, kad pirminiai skaičiai nėra vien tik skaičių teorijos mokslo objektas. Jie nagrinėjami ir kitose matematikos šakose. Kartais ir apibrėžiami labai neįprastai. Štai kokia rekurentinė pirminių skaičių p_i apibrėžimo formulė kombinatorikoje:

$$p_{n+1}=\left[1-\log_2\left(\frac{1}{2}+\sum_{r=1}^{n}\sum_{1\leqslant i_1\leqslant\ldots\leqslant i_r\leqslant n}\frac{(-1)^r}{2^{p_{i_1}\cdots p_{i_r}}-1}\right)\right]$$

(laužtiniai skliaustai reiškia skaičiaus sveikąją dalį, kaip ir § 1). O lošimų teorijoje pirminiai skaičiai taip apibrėžiami. Imama 14 racionaliųjų skaičių:

$$\frac{17}{91},\ \frac{78}{85},\ \frac{19}{51},\ \frac{23}{38},\ \frac{29}{33},\ \frac{77}{29},\ \frac{95}{23},\ \frac{77}{19},\ \frac{1}{17},\ \frac{11}{13},\ \frac{13}{11},\ \frac{15}{14},\ \frac{15}{2},\ 55.$$

Pirmasis sekos skaičius yra $N_1=2$. Skaičius N_2 gaunamas N_1 dauginant iš užrašytų racionaliųjų skaičių. Pirmoji sandauga, kuri lygi sveikajam skaičiui, laikoma lygia N_2. Panašiai randamas N_3 ir t. t. Gaunama tam tikra seka N_i, kurios pirmieji skaičiai šitokie: 2, 15, 825, 725, 1925, ... Šioje sekoje yra ir dvejeto laipsnių 2^p ($p>1$). Visi tų laipsnių rodikliai p yra pirminiai skaičiai, einantys tokia pat tvarka kaip ir natūrinių skaičių sekoje.

Dar vieną pirminių skaičių radimo būdą, kilusį iš matematinės logikos, paminėsime kitame paragrafe.

63. Kurie iš skaičių n, $2600<n<2700$, yra pirminiai?

64. Nustatykite, ar pirminiai yra skaičiai 5927, 5929, 5931, 5937, 5939, 5941, 5943, 5963.

65. Įrodykite, kad nelyginio skaičiaus kvadratą dalydami iš 8 gauname liekaną 1.

66. Įrodykite, kad skaičiai $3n+2$ ($n\in\mathbb{N}$) nėra sveikųjų skaičių kvadratai.

67. Įrodykite, kad skaičius m^2+2 yra pirminis, kai pirminiai yra skaičiai m ir m^2-2.

68. Įrodykite, kad dalydami pirminio skaičiaus $p>5$ kvadratą iš 24 gauname liekaną 1.

69. Raskite visus tokius natūrinius skaičius n^2+1, kurie dalijasi iš $n+1$.

70. Raskite, su kuriomis a reikšmėmis visi skaičiai a, $a+4$, $a+14$ yra pirminiai.

71. Įrodykite, kad $4p+1$ — sudėtinis skaičius, kai $p>5$ ir $2p+1$ — pirminiai skaičiai.

72. Įrodykite, kad skaičiai $mn\,(m^4-n^4)$ ir m^5-m dalijasi iš 30.

73. Įrodykite, kad skaičiai $n\,(n+1)\,(n+2)$, $n\,(n^2+5)$ ir $n\,(n+1)\,(2n+1)$ dalijasi iš 6.

74. Įrodykite, kad skaičiai $4^n+15n-1$ ($n\in\mathbb{N}$) dalijasi iš 9.

75. Įrodykite, kad 5 iš eilės einančių sveikųjų skaičių kvadratų suma nėra natūrinio skaičiaus kvadratas.

76. Įrodykite, kad $(n+1)^n-1$ dalijasi iš n^2.

77. Įrodykite, kad pirminio skaičiaus dalybos iš 30 liekana yra taip pat pirminis skaičius arba 1.

78. Įrodykite, kad skaičiai $2^{2^m}+1$, $2^{2^n}+1$ yra tarpusavyje pirminiai, kai $m\neq n$.

79. Įrodykite, kad du nelyginiai skaičiai yra tarpusavyje pirminiai, jeigu jų skirtumas lygus 2^n.

80. Remdamiesi antruoju Oilerio kriterijumi, įrodykite, kad su visais natūriniais skaičiais m ir n skaičius $N=n^4+4m^4$ yra sudėtinis.

81. Skaičiai 2^p-1 ir 2^q-1 yra tarpusavyje pirminiai. Įrodykite, kad p ir q — tarpusavyje pirminiai.

82. Jeigu skaičiai m ir n tarpusavyje pirminiai, tai skaičių $m+n$ ir m^2+n^2 d.b.d. yra 1 arba 2.

83. Raskite skaičių, kurio pirminiai dalikliai yra tik 2 ir 3, o jo kubo visų daliklių skaičius 7 kartus didesnis už ieškomojo skaičiaus daliklių skaičių.

84. Įrodykite, kad $2^{2n}+2^n+1$ dalijasi iš 7, kai n nėra skaičiaus 3 kartotinis.

85. Tarkime, kad p — pirminis skaičius, $n\in\mathbb{N}$. Įrodykite, kad n^p-n dalijasi iš p. Jeigu n nesidalija iš p, tai $n^{p-1}-1$ dalijasi iš p (*Mažoji Ferma teorema*).

86. Įrodykite, kad $(a+b)^p-(a^p+b^p)$ dalijasi iš p, jei a ir b — sveikieji skaičiai, o p — pirminis.

87. Kokios turi būti natūrinio skaičiaus n reikšmės, jei $n^{n+1}-(n+1)^n$ dalijasi iš 3?

§11. Pagrindinė aritmetikos teorema. Kanoninis skaidinys

Pagrindinė aritmetikos teorema. Nemažai sveikųjų skaičių savybių mums atrodo gana paprastos, akivaizdžios, netgi trivialios. Tačiau nagrinėdami bendresnes struktūras (žiedus, grupes, laukus), kai kuriose iš jų pasigendame tam tikrų savybių, būdingų sveikiesiems skaičiams. Todėl kiek kitaip imame vertinti ir atitinkamas sveikųjų skaičių savybes. Viena iš tokių gana svarbių (bendresniu požiūriu) savybių yra skaičiaus išraiškos pirminių daugiklių sandauga vienatis. Ši savybė vadinama *pagrindine aritmetikos teorema.*

16 (pagrindinė aritmetikos) teorema. *Kiekvienas sudėtinis skaičius vieninteliu būdu (neatsižvelgiant į daugiklių tvarką) išreiškiamas pirminių skaičių sandauga.*

Įrodymas. Pradžioje įrodysime, kad tokia išraiška galima, po to — kad ji vienintelė.

1. Jeigu n yra sudėtinis skaičius, tai (14 teoremos 3 išvada) jis turi pirminį daliklį p. Taigi $n=pm$. Jeigu m taip pat pirminis, tai skaičius n yra išreikštas dviejų pirminių skaičių sandauga. Jeigu m yra sudėtinis skaičius, toliau skaidome m. Kadangi $1<m<n$, tai kiekvieną kartą tenka skaidyti vis mažesnius natūrinius skaičius. Akivaizdu, kad tas skaidymo procesas anksčiau ar vėliau užsibaigs ir skaičius n bus pirminių skaičių sandauga

$$n=p_1p_2\ldots p_r.$$

2. Tarkime, kad ne visi sudėtiniai skaičiai vienintelių būdu išskaidomi į pirminius daugiklius. Sakykime, a yra mažiausias sudėtinis skaičius, išskaidomas nevienareikšmiškai:

$$a=p_1p_2\ldots p_k=h_1h_2\ldots h_s; \tag{1.27}$$

čia visi p ir h – pirminiai skaičiai.

Atkreipsime dėmesį, kad nė vienas iš skaičių p (1.27) lygybėje nėra lygus jokiam pirminiam skaičiui h. Priešingu atveju, suprastinę abi (1.27) lygybės puses iš to pirminio p, gautume, kad dar mažesnis už a skaičius a/p išskaidomas nevienareikšmiškai.

Parinkime abiejose (1.27) lygybės pusėse po vieną pirminį skaičių, pavyzdžiui, p_1 ir h_1. Visų kitų pirminių skaičių sandaugas atitinkamai žymėkime raidėmis b ir c:

$$a=p_1b=h_1c.$$

Matėme, kad $p_1\neq h_1$. Tarkime, jog $p_1>h_1$ (priešingas atvejis nagrinėjamas analogiškai). Padaliję p_1 iš h_1 su liekana (2 teorema), gauname

$$p_1=qh_1+r, \quad 0\leqslant r<h_1.$$

Tuomet

$$a=p_1b=(qh_1+r)b=qh_1b+rb=h_1c,$$

$$rb=h_1c-qh_1b=h_1(c-qb).$$

Pažymėję skirtumą $c-qb$ raide g ir įrašę į pastarąją lygybę b išraišką, turime

$$rp_2p_3\ldots p_k=h_1g.$$

Nesunku pastebėti, kad ta lygybė reiškia nevienareikšmį skaidinį į pirminius skaičius. Iš tiesų pirminis skaičius h_1 nelygus nė vienam kairiosios pusės pirminiam daugikliui $p_2, p_3, \ldots, p_k$ (tai jau aptarėme). Skaičius h_1 nėra ir r daliklis ($r<h_1$). Baigę skaidyti į pirminius daugiklius skaičius r ir g, gausime nevienareikšmį skaičiaus $rp_2p_3\ldots p_k$ skaidinį į pirminius daugiklius. Bet tai prieštarauja prielaidai, kad a – mažiausias nevienareikšmiškai išskaidomas skaičius, nes

$$r<h_1\Rightarrow r<p_1\Rightarrow rp_2p_3\ldots p_k<p_1p_2\ldots p_k=a.$$

Teorema įrodyta.

Visa sveikųjų skaičių dalumo teorija iš esmės paremta pagrindine aritmetikos teorema. Ta teorema nėra triviali. Tuo įsitikinsime kituose skyriuose nagrinėdami tokį žiedą, kuriame analogiška teorema nėra teisinga.

Kanoninis skaidinys. Įrodėme, kad bet kurį sudėtinį skaičių $n>1$ galima išreikšti pirminių skaičių sandauga:

$$n=p_1p_2\cdot\ldots\cdot p_r.$$

Tuos daugiklius toliau lygiagrečiai vadinsime taip pat ir *dalikliais*. Terminas „daliklis“ labiau pažymi tai, kad iš skaičių p_i dalijasi n, o žodis „daugiklis“ – kad visų tų skaičių sandauga lygi n.

Skaičiaus skaidinyje gali būti ir sutampančių pirminių daugiklių. Pakeitę jų sandaugas laipsniais, gausime išraišką

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}, \tag{1.28}$$

kurioje visi laipsnių pagrindai yra skirtingi pirminiai skaičiai, o rodikliai – natūriniai skaičiai. Tokią skaičiaus n išraišką vadiname *kanoniniu skaidiniu.*

Pavyzdys. Skaičių 4200 išskaidę į pirminius daugiklius, gausime $4200=2\cdot2\cdot2\cdot3\cdot5\cdot5\cdot7$. To skaičiaus kanoninis skaidinys yra $4200=2^3\cdot3\cdot5^2\cdot7$.

Teoriniuose nagrinėjimuose patogu naudotis glaustai užrašyta lygybe

$$n=\prod_{p\mid n}p^{\alpha_p}.$$

Pastaroji išraiška rodo, kad dauginame tiek skirtingų laipsnių p^{α_p}, kiek yra skirtingų pirminių skaičiaus n daliklių. Kiekvieną tokį pirminį p atitinka tam tikras rodiklis α_p. Kartais paprastumo dėlei praleisime indeksą p ir rašysime tik α, turėdami omenyje, kad tas α kiekvienam pirminiam skaičiui gali būti kitas. Skaičiaus 1 ir pirminių skaičių kanoniniai skaidiniai sutampa su pačiais skaičiais.

Kanoninio skaidinio sąvoką galime taikyti ir nesuprastinamoms trupmenoms, prirašydami prie trupmenos skaitiklio kanoninio skaidinio jos vardiklio skaidinį su neigiamais rodikliais.

Pavyzdžiui,

$$\frac{120}{49}=\frac{2^3\cdot3\cdot5}{7^2}=2^3\cdot3\cdot5\cdot7^{-2}.$$

Taigi skaičius $n=\prod_{p\mid n}p^{\alpha}$ yra sveikasis, jei visi jo rodikliai α – neneigiami sveikieji skaičiai.

Kartais patogu operuoti skaidiniais, kuriuose yra ne tik n dalikliai, bet ir visi be išimties pirminiai skaičiai. Tokius skaidinius gauname prie sandaugos prirašę visus trūkstamus pirminius skaičius su nuliniais rodikliais.

Pavyzdžiui,

$$1400=2^3\cdot5^2\cdot7=2^3\cdot3^0\cdot5^2\cdot7\cdot11^0\cdot13^0\cdot17^0\ldots$$

Analogiškai galime pakeisti ir (1.28) formulę:

$$n=\prod_{p}p^{\alpha}.$$

Toje formulėje sandauga yra begalinė, nes dauginami visų pirminių skaičių laipsniai, tačiau yra tik baigtinis skaičius teigiamų rodiklių α_0; visų tų pirminių skaičių, iš kurių nesidalija n, rodikliai lygūs 0.

Ieškodami skaičiaus n kanoninio skaidinio, pirmiausia randame visus jo pirminius daugiklius. To uždavinio sprendimas ir vadinamas skaičiaus *n faktorizacija* (anglų kalbos žodis „factor" reiškia daugiklį). Daug matematikų ieškojo tinkamų skaičių faktorizacijos metodų, tačiau kol kas universalaus, spartaus ir patogaus metodo nėra. Visi žinomi faktorizacijos metodai turi vienokių ar kitokių trūkumų, visi jie nepatogūs, kai reikia faktorizuoti didelius skaičius.

Kaip pavyzdį, išnagrinėsime vieną iš faktorizacijos būdų.

17 teorema. *Nelyginis skaičius* $n \geqslant 9$ *tada ir tik tada yra sudėtinis, kai tarp skaičių*

$$N_0=n,\ N_1=N_0+1,\ N_2=N_1+3,\ \ldots,\ N_s=N_{s-1}+2s-1$$

$$\left(1 \leqslant s \leqslant \left[\frac{n-9}{6}\right]\right)$$

yra kvadratas

$$N_s=t^2 \Leftrightarrow n=(t-s)(t+s).$$

Įrodymas. Kadangi

$$N_s=n+1+3+\ldots+2s-1=n+s^2,$$

tai iš lygybės $N_s=n+s^2=t^2$ išplaukia $n=(t-s)(t+s)$. Lieka patikrinti, ar $t-s$ yra netrivialusis daliklis, t. y. didesnis už 1:

$$s \leqslant \left[\frac{n-9}{6}\right] \Rightarrow s \leqslant \frac{n-9}{6} \Rightarrow n \geqslant 6s+9 \Rightarrow n > 2s+1 \Rightarrow$$

$$\Rightarrow t^2=n+s^2 > 2s+1+s^2=(s+1)^2 \Rightarrow t > s+1 \Rightarrow t-s > 1.$$

Įrodysime sąlygos būtinumą. Jeigu $n=ab$ yra nelyginio skaičiaus skaidinys į du netrivialiuosius daugiklius, pavyzdžiui, $a \leqslant b$, tai

$$3 \leqslant a \leqslant \sqrt{n},\ \sqrt{n} \leqslant b \leqslant \frac{n}{3}.$$

Tuomet, imdami $s=\frac{b-a}{2}$, gauname

$$N_s=n+s^2=ab+\left(\frac{b-a}{2}\right)^2=ab+\frac{b^2}{4}-\frac{ab}{2}+\frac{a^2}{4}=\left(\frac{b+a}{2}\right)^2.$$

Be to,

$$0 \leqslant \frac{b-a}{2} \leqslant \frac{1}{2}\left(\frac{n}{3}-3\right)=\frac{n-9}{6}.$$

Pavyzdys. Išskaidysime skaičių 221. Turime: $N_0=221$, $N_1=222$, $N_2=225=15^2$. Todėl $221=(15-2)(15+2)=13 \cdot 17$.

Ši teorema paremta pirmuoju Oilerio kriterijumi, apie kurį kalbėjome praeitame paragrafe.

18 teorema. *Jeigu skaičiaus n kanoninis skaidinys yra*

$$n=\prod_{p \mid n} p^{\alpha_p},$$

tai skaičiaus n bet kurio daliklio d kanoninis skaidinys yra šitoks:

$$d = \prod_{p \mid n} p^{\beta_p};$$

čia

$$0 \leqslant \beta_p \leqslant \alpha_p.$$

Įrodymas. Iš 5 dalumo savybės išplaukia, kad skaičiaus n daliklių kanoniniuose skaidiniuose negali būti tokių pirminių daugiklių, kurių nėra skaičiaus n skaidinyje. Lieka įsitikinti, kad d kanoniniame skaidinyje bet kuris pirminis daugiklis p negali būti aukštesnio laipsnio negu skaičiaus n kanoniniame skaidinyje.

Iš $d \mid n$ išplaukia $n = dt$ $(t \in \mathbf{N})$, todėl

$$\prod_{p \mid n} p^{\alpha_p} = t \prod_{p \mid n} p^{\beta_p}.$$

Taigi

$$t = \prod_{p \mid n} p^{\alpha_p - \beta_p}.$$

Skaičius t yra sveikasis, tad jo kanoniniame skaidinyje visi rodikliai turi būti neneigiami, t. y.

$$\alpha_p - \beta_p \geqslant 0 \Rightarrow \beta_p \leqslant \alpha_p.$$

Teorema įrodyta.

Pavyzdys. Remdamiesi ta teorema, rasime visus skaičiaus $135 = 3^3 \cdot 5$ daliklius. Šiuo atveju

$$d = \prod_{p \mid 135} p^{\beta_p}.$$

Kadangi 135 dalijasi tik iš dviejų pirminių skaičių 3 ir 5, tai

$$d = 3^{\beta_3} \cdot 5^{\beta_5};$$

čia

$$0 \leqslant \beta_3 \leqslant 3,$$
$$0 \leqslant \beta_5 \leqslant 1.$$

Sudarę visas galimas rodiklių β_3 ir β_5 reikšmių kombinacijas nurodytose ribose, gauname

$$d_1 = 3^0 \cdot 5^0 = 1, \quad d_2 = 3^1 \cdot 5^0 = 3,$$
$$d_3 = 3^2 \cdot 5^0 = 9, \quad d_4 = 3^3 \cdot 5^0 = 27,$$
$$d_5 = 3^0 \cdot 5^1 = 5, \quad d_6 = 3^1 \cdot 5^1 = 15,$$
$$d_7 = 3^2 \cdot 5^1 = 45, \quad d_8 = 3^3 \cdot 5^1 = 135.$$

Taigi skaičius 135 turi 8 daliklius.

Remdamiesi šia teorema, galime rasti kelių skaičių d. b. d. ir m. b. k. kanoninius skaidinius, kai žinomi tų skaičių skaidiniai.

19 teorema. *Sakykime, skaičių* $a_1, a_2, \ldots, a_n$ *kanoniniai skaidiniai yra*

$$a_i = \prod_p p^{\alpha_p^{(i)}}, \quad i = 1, 2, \ldots, n.$$

Tada jų didžiausio bendrojo daliklio d *ir mažiausio bendrojo kartotinio* b *kanoniniai skaidiniai yra*

$$d = (a_1, a_2, \ldots, a_n) = \prod_p p^{\alpha_p},$$

$$b = [a_1, a_2, \ldots, a_n] = \prod_p p^{\gamma_p};$$

čia

$$\alpha_p = \min\{\alpha_p^{(1)}, \alpha_p^{(2)}, \ldots, \alpha_p^{(n)}\},$$

$$\gamma_p = \max\{\alpha_p^{(1)}, \alpha_p^{(2)}, \ldots, \alpha_p^{(n)}\}.$$

Įrodymas. Skaičiaus a_i daliklio kanoniniame skaidinyje pirminio daugiklio p laipsnio rodiklis gali būti ne didesnis už atitinkamą rodiklį $\alpha_p^{(i)}$. Taigi į kiekvieno iš skaičių $a_1, a_2, \ldots, a_n$ bendrojo daliklio kanoninį skaidinį p įeina su laipsnio rodikliu β_p, ne didesniu už mažiausią iš tų rodiklių:

$$\beta_p \leqslant \min\{\alpha_p^{(1)}, \alpha_p^{(2)}, \ldots, \alpha_p^{(n)}\} = \alpha_p.$$

Akivaizdu, kad į skaičių $a_1, a_2, \ldots, a_n$ didžiausio bendrojo daliklio kanoninį skaidinį p turi įeiti su didžiausiu galimu rodikliu α_p.

Tarkime, kad skaičių $a_1, a_2, \ldots, a_n$ mažiausio bendrojo kartotinio b kanoninis skaidinys yra

$$b = \prod_p p^{\gamma_p}.$$

Kadangi skaičiai a_i yra skaičiaus b dalikliai, tai (žr. 18 teoremą) gauname nelygybes

$$\begin{aligned} \alpha_p^{(1)} &\leqslant \gamma_p, \\ \alpha_p^{(2)} &\leqslant \gamma_p, \\ &\cdots\cdots \\ \alpha_p^{(n)} &\leqslant \gamma_p, \end{aligned}$$

ekvivalenčias vienai nelygybei

$$\max(\alpha_p^{(1)}, \alpha_p^{(2)}, \ldots, \alpha_p^{(n)}) = \max_{1 \leqslant i \leqslant n} \alpha_p^{(i)} \leqslant \gamma_p.$$

Mažiausią bendrąjį kartotinį gausime paėmę mažiausias galimas visų rodiklių γ_p reikšmes

$$\max_{1 \leqslant i \leqslant n} \alpha_p^{(i)}.$$

Teorema įrodyta.

Pavyzdys. Rasime skaičių $a_1=24$, $a_2=180$, $a_3=450$ d.b.d. ir m.b.k. kanoninius skaidinius.

Kadangi $24=2^3\cdot 3$, $180=2^2\cdot 3^2\cdot 5$, $450=2\cdot 3^2\cdot 5^2$, tai

$$\alpha_2=\min\{\alpha_2^{(1)}, \alpha_2^{(2)}, \alpha_2^{(3)}\}=\min\{3, 2, 1\}=1,$$
$$\alpha_3=\min\{\alpha_3^{(1)}, \alpha_3^{(2)}, \alpha_3^{(3)}\}=\min\{1, 2, 2\}=1,$$
$$\alpha_5=\min\{\alpha_5^{(1)}, \alpha_5^{(2)}, \alpha_5^{(3)}\}=\min\{0, 1, 2\}=0.$$

Likusieji α_p lygūs nuliui, nes kiti pirminiai skaičiai neįeina į nagrinėjamų skaičių kanoninius skaidinius. Todėl

$$d=(24, 180, 450)=\prod_p p^{\alpha_p}=2^{\alpha_2}3^{\alpha_3}5^{\alpha_5}=2^1\cdot 3^1\cdot 5^0=6.$$

Toliau gauname

$$\gamma_2=\max\{\alpha_2^{(1)}, \alpha_2^{(2)}, \alpha_2^{(3)}\}=\max\{3, 2, 1\}=3,$$
$$\gamma_3=\max\{\alpha_3^{(1)}, \alpha_3^{(2)}, \alpha_3^{(3)}\}=\max\{1, 2, 2\}=2,$$
$$\gamma_5=\max\{\alpha_5^{(1)}, \alpha_5^{(2)}, \alpha_5^{(3)}\}=\max\{0, 1, 2\}=2.$$

Todėl

$$b=[24, 180, 450]=\prod_p p^{\gamma_p}=2^3\cdot 3^2\cdot 5^2=1800.$$

Šis d. b. d. ir m. b. k. radimo būdas dėstomas ir vidurinėje mokykloje.

Faktorizuojant skaičius, buvo mėginama naudotis funkcijomis, kurių reikšmės tam tikrame intervale yra pirminiai arba sudėtiniai skaičiai. Pavyzdžiui, funkcijos n^4+4 reikšmės visuomet yra sudėtiniai skaičiai, jei $n>1$. Iš tiesų

$$n^4+4=(n^2+2n+2)(n^2-2n+2).$$

Buvo mėginama naudotis ir kitokio pavidalo funkcijomis – daugianariais. Dar L. Oileris nurodė, kad daugianario n^2-n+41 reikšmės yra pirminiai skaičiai, kai $n=0, 1, 2, \ldots, 39, 40$. Daugianario $n^2-79n+1601$ reikšmės yra pirminiai skaičiai, kai n – sveikasis skaičius, $0\leqslant n\leqslant 79$. Funkcijos n^3+1 tik viena reikšmė (kai $n=1$) yra pirminis skaičius, tačiau manoma, kad yra be galo daug $n^3\pm 2$ pavidalo pirminių skaičių.

1962 m. *M. Bredichinas* įrodė, kad yra be galo daug pirminių n^2+m^2+1 pavidalo skaičių.

Panašių faktorizacijos rezultatų gauta ir daugiau, tačiau visi jie susiję su atskiromis problemomis, toli gražu ne universalūs. Šiuo požiūriu labai įdomus tarybinio matematiko *J. Matijasevičiaus* neseniai gautas rezultatas sprendžiant 10-ąją *Hilberto problemą*. (Žymus vokiečių matematikas *D. Hilbertas* (D. Hilbert, 1862–1943), 1893–1895 m. profesoriavęs Karaliaučiaus universitete, 1900 m. tarptautiniame matematikų kongrese Paryžiuje iškėlė 23 problemas iš įvairių matematikos sričių, kurios išryškino XIX a. pabaigos matematikos pagrindines tendencijas. Šios problemos buvo pavadintos Hilberto vardu. Ne visos jos išspręstos iki šiol.)

J. Matijasevičius rado tokį 26 kintamųjų daugianarį, kurio visos teigiamos reikšmės, kai kintamieji įgyja sveikąsias reikšmes, sutampa su pirminių skaičių aibe. Tas daugianaris

$$F(a,\ b,\ c,\ d,\ e,\ f,\ g,\ h,\ i,\ j,\ k,\ l,\ m,\ n,\ o,\ p,\ q,\ r,\ s,$$

$$t,\ u,\ v,\ w,\ x,\ y,\ z)$$

yra 25-ojo laipsnio; jam užrašyti, kaip matote, prireikė visos lotyniškosios abėcėlės.

Norėdami parodyti jo struktūrą, užrašysime porą pabaigos narių:

$$\ldots -(a^2l^2-l^2+1-m^2)^2-(n+l+v-y)^2.$$

Uždaviniai

88. Užrašykite skaičių 2400, 2401, 2402, 2404, 2410 kanoninius skaidinius.

89. Užrašykite skaičių 16 200, 41 067, 82 798 848 kanoninius skaidinius.

90. Naudodamiesi kanoniniais skaidiniais, raskite (96, 142), (720, 504), (252, 660), (126, 525), (187, 533, 317).

91. Remdamiesi 18 teorema ir Euklido algoritmu, raskite šiuos mažiausius bendruosius kartotinius: [42, 82], [35, 120], [24, 34, 48], [35, 90, 125], [16, 40, 82, 90].

92. Naudodamiesi kanoniniais skaidiniais, raskite [48, 90], [62, 120], [45, 95, 125], [75, 220, 310].

93. Raskite skaičiaus n daliklių sandaugą.

94. Raskite skaičių, kurio daliklių sandauga lygi $3^{30}\ 5^{40}$.

95. Raskite skaičiaus n^3 daliklių skaičių, kai n^2 turi 15 daliklių, o skaičiaus n kanoninis skaidinys yra tik 2 skirtingų pirminių skaičių laipsnių sandauga.

96. Raskite mažiausią $n=2^\alpha pq$ pavidalo skaičių (p ir q — skirtingi pirminiai skaičiai), kurio daliklių suma būtų lygi $3n$ (*Ferma uždavinys*).

97. Raskite natūrinį skaičių, kuris turi 14 daliklių ir dalijasi iš 3 ir 4.

Įrodykite šiuos teiginius.

98. Jeigu skaičiai a ir b neturi netrivialių bendrųjų daliklių, tai jų sandaugos daliklį d galima išreikšti sandauga $d=d_1d_2$,

$$d_1 \mid a,\ d_2 \mid b.$$

99. Jeigu $d \mid a_1a_2\ldots a_n$ ir kiekviena skaičių $a_1, a_2, \ldots, a_n$ pora neturi bendrųjų daliklių, tai

$$d=d_1d_2\ldots d_n;$$

čia $d_i \mid a_i$ ($i=1, 2, \ldots, n$).

100. Jeigu skaičiai a ir b yra tarpusavyje pirminiai, o jų sandauga lygi sveikojo skaičiaus natūriniam laipsniui

$$ab=c^n,$$

tai $a=a_1^n$, $b=b_1^n$; čia a_1 ir b_1 — sveikieji skaičiai.

101. Jeigu skaičius dalijasi iš kelių tarpusavyje pirminių skaičių, tai jis dalijasi ir iš jų sandaugos.

102. Dvi nesuprastinamos trupmenos lygios tada ir tik tada, kai atitinkamai lygūs jų skaitikliai ir vardikliai.

103. n-ojo laipsnio šaknis iš natūrinio skaičiaus m yra sveikasis skaičius tada ir tik tada, kai skaičiaus m kanoninio skaidinio visų pirminių daugiklių laipsniai dalijasi iš n.

104. Įrodykite 12 teoremą remdamiesi skaičių a ir b kanoniniais skaidiniais.

105. Nustatykite, keliais būdais skaičių n galima išreikšti dviejų dauginamųjų sandauga, kai skaičiaus n kanoninis skaidinys yra

$$n=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}.$$

§12. Skaičiaus natūrinių daliklių skaičius ir suma

Žinodami natūrinio skaičiaus n kanoninį skaidinį, galime užrašyti visus to skaičiaus daliklius, nustatyti jų skaičių. Daliklių skaičius yra funkcija, pasižyminti įdomiomis savybėmis.

Išsiaiškinsime *aritmetinės funkcijos* sąvoką.

Aritmetinėmis dažniausiai vadinamos funkcijos, kurios apibrėžtos sveikųjų skaičių aibėje arba kurių reikšmės yra sveikieji skaičiai. Pavyzdžiui, anksčiau minėta Oilerio funkcija $\varphi(n)$, išreiškianti skaičių natūrinių skaičių, ne didesnių už n ir tarpusavyje pirminių su n, yra aritmetinė funkcija. Prie aritmetinių funkcijų priskiriama ir sveikoji skaičiaus x dalis — funkcija $[x]$ bei trupmeninė skaičiaus x dalis — funkcija $\{x\}$. Nors funkcija $[x]$ apibrėžta realiųjų skaičių aibėje, tačiau jos reikšmės yra sveikieji skaičiai. Funkcijos $\{x\}$ reikšmės nėra vien sveikieji skaičiai, ši funkcija apibrėžta ne vien sveikosioms argumento reikšmėms, bet ji priskiriama prie aritmetinių funkcijų dėl savo glaudaus ryšio su aritmetika, skaičių teorija.

Svarbią aritmetinių funkcijų klasę sudaro *multiplikatyviosios aritmetinės funkcijos.*

Multiplikatyviąja aritmetine funkcija vadiname vieno argumento funkciją $f(n)$, tenkinančią sąlygą

$$f(mn)=f(m)f(n) \tag{1.29}$$

su bet kuria tarpusavyje pirminių skaičių m, n pora.

Multiplikatyviąsias aritmetines funkcijas toliau vadinsime trumpiau — *multiplikatyviosiomis funkcijomis.*

Jeigu aritmetinei funkcijai (1.29) lygybė galioja ne tik su tarpusavyje pirminių skaičių m ir n poromis, bet su visomis sveikųjų skaičių m ir n poromis, tai tokią funkciją vadiname *visiškai multiplikatyvia.* Tuo atveju

$$f(p^\alpha)=[f(p)]^\alpha$$

su visais pirminiais skaičiais p, $\alpha\in\mathbf{N}$.

Jeigu vietoje pastarosios lygybės teisinga lygybė

$$f(p^\alpha)=f(p)$$

su visais pirminiais skaičiais p ($\alpha\in\mathbf{N}$), tai funkcija $f(n)$ vadinama *stipriai multiplikatyvia.*

Paprasčiausias multiplikatyviosios funkcijos pavyzdys yra laipsninė funkcija $f(m)=m^a$. Iš tikrųjų

$$f(mn)=(mn)^a=m^a n^a=f(m)f(n).$$

Taigi ta funkcija yra visiškai multiplikatyvi.

Natūrinio skaičiaus n natūrinių daliklių skaičių žymėsime $\tau(n)$. Tai natūrinio argumento funkcija, jai teisinga šitokia teorema.

20 teorema. *Funkcija* $\tau(n)$ — *multiplikatyvi.*

Įrodymas. Tarkime, kad $(m, n)=1$. Nesunku nustatyti (žr., pavyzdžiui, 98 uždavinį), kad bet kurį skaičiaus mn daliklį d galima išreikšti sandauga: $d=d_1d_2$; čia $d_1 \mid m$, $d_2 \mid n$. Skaičius m turi $\tau(m)$, o skaičius n — $\tau(n)$ skirtingų pirminių daliklių. Funkciją $\tau(n)$ galima užrašyti šitaip:

$$\tau(n)=\sum_{d \mid n} 1.$$

Todėl

$$\tau(mn)=\sum_{d \mid mn} 1=\sum_{\substack{d_1 \mid m \\ d_2 \mid n}} 1=\Big(\sum_{d_1 \mid m} 1\Big)\Big(\sum_{d_2 \mid n} 1\Big).$$

Taigi $\tau(mn)=\tau(m)\,\tau(n)$.

Žinodami skaičiaus n kanoninį skaidinį ir remdamiesi ką tik įrodyta savybe, nesunkiai apskaičiuosime $\tau(n)$.

21 teorema. *Jeigu* $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, *tai*

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1). \tag{1.30}$$

Įrodymas. Iš $\tau(n)$ multiplikatyvumo išplaukia, kad

$$\tau(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k})=\tau(p_1^{\alpha_1})\,\tau(p_2^{\alpha_2})\dots\tau(p_k^{\alpha_k}). \tag{1.31}$$

Skaičiaus p^α dalikliai yra tik šie p laipsniai:

$$1,\ p,\ p^2,\ \dots,\ p^{\alpha-1},\ p^\alpha.$$

Taigi

$$\tau(p^\alpha)=(\alpha+1).$$

Iš čia ir iš (1.31) lygybės gauname (1.30) formulę.

Skaičiuodami funkcijos $\tau(n)$ reikšmes iš eilės einantiems natūriniams skaičiams n, nepastebime jokio dėsningumo tų reikšmių pasiskirstyme. Dėsningumas išryškėja tik tiriant tų reikšmių vidurkius. Pateiksime įdomią tuos vidurkius apibūdinančią formulę:

$$\frac{1}{n}\sum_{k=1}^{n}\tau(k)=\ln n+2C-1+r(n);$$

čia C — vadinamoji Oilerio konstanta:

$$C=0{,}577215664901532\dots,$$

$$|r(n)|\leqslant\frac{a}{\sqrt{n}},$$

a — tam tikra konstanta. Taigi

$$\lim_{n\to\infty}\left(\frac{1}{n}\sum_{k=1}^{n}\tau(n)-\ln n\right)=2C-1.$$

Pavyzdžiai. 1. Žinome, kad skaičius 135 turi 8 daliklius. Iš tikrųjų, kadangi $135=3^3\cdot 5$, tai

$$\tau(135)=(3+1)(1+1)=8.$$

2. Rasime $\tau(2800)$. Skaičiaus 2800 kanoninis skaidinys yra $2^4\cdot 5^2\cdot 7$, todėl

$$\tau(2800)=(4+1)(2+1)(1+1)=30.$$

Pirminiai skaičiai p išsiskiria iš kitų natūrinių skaičių savybe

$$\tau(p)=2.$$

Visų sudėtinių skaičių n daliklių skaičius $\tau(n)>2$, o $\tau(1)=1$.

Nagrinėsime dar vieną aritmetinę funkciją — visų skaičiaus n daliklių a-ųjų laipsnių sumą. Ta suma žymima

$$\sigma_a(n)=\sum_{d\mid n} d^a. \tag{1.32}$$

Įrodysime šitokią teoremą.

22 teorema. *Funkcija $\sigma_a(n)$ yra multiplikatyvi.*

Įrodymas. Jeigu $(m, n)=1$, tai kiekvieną sandaugos mn daliklį d galima išreikšti sandauga

$$d=d_1d_2;$$

čia $d_1\mid m$, $d_2\mid n$. Įrašę tą išraišką į (1.32), gauname

$$\sigma_a(mn)=\sum_{\substack{d_1\mid m\\ d_2\mid n}}(d_1d_2)^a=\sum_{d_1\mid m}\sum_{d_2\mid n}d_1^a d_2^a=\sum_{d_1\mid m}d_1^a\sum_{d_2\mid n}d_2^a=\sigma_a(m)\,\sigma_a(n).$$

Iš tikrųjų, jeigu d_1 įgyja visų skaičiaus m daliklių reikšmes, d_2 — visų skaičiaus n daliklių reikšmes, tai sandauga d_1d_2 įgyja visų sandaugos mn daliklių reikšmes.

23 teorema. *Jeigu natūrinio skaičiaus n kanoninis skaidinys yra*

$$n=\prod_{p\mid n}p^{\alpha},$$

tai

$$\sigma_a(n)=\prod_{p\mid n}\frac{p^{(\alpha+1)a}-1}{p^a-1}.$$

Įrodymas. Kadangi $\sigma_a(n)$ – multiplikatyvioji funkcija, tai

$$\sigma_a(n)=\sigma_a(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k})=\sigma_a(p_1^{\alpha_1})\,\sigma_a(p_2^{\alpha_2})\ldots\sigma_a(p_k^{\alpha_k})=\prod_{p\mid n}\sigma_a(p^{\alpha}).$$

Tačiau

$$\sigma_a(p^{\alpha})=1+p^a+p^{2a}+\ldots+p^{(\alpha-1)a}+p^{\alpha a}=\frac{p^{(\alpha+1)a}-1}{p^a-1}.$$

Išvada. *Pažymėję skaičiaus* $n=\Pi\,p^{\alpha}$ *daliklių sumą* $\sigma_1(n)=\sigma(n)$, *turime*

$$\sigma(n)=\prod_{p\mid n}\frac{p^{\alpha+1}-1}{p-1}.$$

Pavyzdžiai. 1. Rasime skaičiaus 24 daliklių kvadratų sumą. Pritaikę įrodytąją formulę, kai $a=2$, randame

$$\sigma_2(24)=\sigma_2(2^3\cdot 3)=\frac{2^{4\cdot 2}-1}{2^2-1}\cdot\frac{3^{2\cdot 2}-1}{3^2-1}=85\cdot 10=850.$$

2. Rasime skaičiaus 28 daliklių sumą:

$$\sigma(28)=\sigma(2^2\cdot 7)=\frac{2^3-1}{2-1}\cdot\frac{7^2-1}{7-1}=7\cdot 8=56.$$

Skaičiai n, kurių

$$\sigma(n)=2n,$$

matematikos istorijoje žinomi *tobulųjų skaičių* pavadinimu. Jeigu $\sigma'(n)$ žymėsime sumą skaičiaus n daliklių, mažesnių už n, tai gausime

$$\sigma'(n)=\sigma(n)-n.$$

Tobulieji skaičiai kaip tik ir yra tie skaičiai, kurių $\sigma'(n)=n$, t. y. jie lygūs sumai visų savo daliklių, mažesnių už juos pačius. Matyt, todėl tie skaičiai ir buvo pavadinti tobulaisiais.

Pirmasis tobulasis skaičius yra 6. Iš tikrųjų to skaičiaus $\sigma'(6)=1+2+3=6$. Antrasis ir trečiasis tobulieji skaičiai – 28, 496. Dar Euklidas nustatė, kad lyginius tobuluosius skaičius n galima rasti iš formulės

$$n=2^{k-1}(2^k-1)=2^{k-1}M_k; \tag{1.33}$$

čia $M_k=2^k-1=p$ – Merseno pirminis skaičius. Iš tikrųjų tokių n

$$\sigma(n)=\sigma(2^{k-1}p)=\frac{2^k-1}{2-1}\cdot\frac{p^2-1}{p-1}=(2^k-1)(p+1)=2^kp=2n.$$

L. Oileris įrodė, kad taikydami Euklido (1.33) formulę galime rasti visus galimus lyginius tobuluosius skaičius. Kiekvieną Merseno pirminį skaičių atitinka vienas tobulasis skaičius. Pavyzdžiui, pirmąjį Merseno pirminį skaičių $M_2=3$ atitinka pirmasis tobulasis skaičius 6, antrąjį Merseno pirminį skaičių $M_3=2^3-1=7$ atitinka antrasis tobulasis skaičius 28 ir t. t. Neseniai didžiausias žinomas tobulasis skaičius buvo 14 474 011 154 664 524 427 946 373 126 085 988 481 573 677 491 474 853 889 066 354 349 131 199 152 128; jis atitiko didžiausią tuo metu žinomą Merseno pirminį skaičių $2^{127}-1$. Šiuo metu žinomi 28 tobulieji skaičiai.

Iki šiol nerasta nė vieno nelyginio tobulojo skaičiaus ir nežinia, ar jų apskritai yra. 1973 m. nustatyta, kad tokie skaičiai, jeigu jie yra, turi būti didesni už 10^{50}.

Tobulieji skaičiai turi ir kitų įdomių savybių. Galima įrodyti, pavyzdžiui, kad kiekvienas lyginis tobulasis skaičius $2^{k-1}M_k$, $k>1$, išreiškiamas $2^{\frac{k-1}{2}}$ iš eilės einančių nelyginių skaičių kubų suma:

$$28 = 1^3 + 3^3,$$

$$496 = 1^3 + 3^3 + 5^3 + 7^3$$

ir t. t.

Didžiausias pastaruoju metu žinomas tobulasis skaičius yra

$$(2^{86243} - 1)\, 2^{86242}.$$

Įdomių dalumo savybių turi ir *draugiškieji skaičiai*. Taip vadinami skaičiai m ir n, kai

$$\sigma(m) = \sigma(n) = m + n.$$

Tuos skaičius galima apibūdinti ir kitaip: jeigu m ir n yra draugiškieji skaičiai, tai skaičiaus m daliklių, mažesnių už m, suma lygi antrajam skaičiui n, o skaičiaus n daliklių, mažesnių už n, suma lygi m.

Pirmąją draugiškųjų skaičių porą rado Pitagoras. Tai skaičiai 220 ir 284. Tikrai skaičiaus 220 daliklių, mažesnių už 220, suma yra

$$1 + 2 + 4 + 5 + 10 + 20 + 11 + 22 + 44 + 55 + 110 = 284.$$

Atitinkamai skaičiaus 284 daliklių, mažesnių už tą skaičių, suma lygi

$$1 + 2 + 4 + 71 + 142 = 220.$$

L. Oileris rado 59 draugiškųjų skaičių poras. Vengrų matematikas P. Erdešas 1955 m. nustatė, kad

$$\lim_{x\to\infty} \frac{A(x)}{x} = 0;$$

čia $A(x)$ reiškia draugiškųjų skaičių, ne didesnių už x, porų skaičių.

Vienas iš paskutinių neseniai gautų rezultatų yra draugiškųjų skaičių a ir b pora, kurią 1972 m. surado Amsterdamo matematikas Hermanas te Rile:

$a = 902364653062\ 3313066515\ 5201592687\ 0786444430\ 4548569003$
$8961540360\ 5363719932\ 5828701918\ 5759580345\ 2747004992$
$7532312907\ 0333233826\ 7840675607\ 3892061566\ 6452384945,$

$b = 862593766501\ 4359638769\ 0953818787\ 1666597148\ 4088835777$
$4281383581\ 6831022646\ 6591332953\ 3162256868\ 3649647747$
$2706738497\ 3129580885\ 3683841099\ 1321499127\ 6380031055.$

Skaičius a turi 800 skirtingų daliklių, skaičius b — 3200. Skaičiaus a daliklių $d<a$ suma lygi skaičiui b, ir atvirkščiai.

Šie, kaip ir kiti pavyzdžiai, rodo, kad matematika yra kūrybiškas, nuolat vystomas mokslas, kad jo šios dienos laimėjimai gali jau nebebūti naujausi rytoj.

Beje, skaitytojui gali kilti klausimas – kam viso to reikia, kokia nauda iš tų rezultatų, kam reikalingi, pavyzdžiui, draugiškieji skaičiai?

Į tokį klausimą galima atsakyti Leonardo Oilerio žodžiais: *„Iš visų problemų, kurios nagrinėjamos matematikoje, nėra kitų tokių, kurios atrodytų tokios nenaudingos kaip skaičių teorijos problemos... Tačiau matematika tikriausiai niekada nebūtų pasiekusi dabarties aukštumų, jei būtų buvusios ignoruojamos ir tos nevaisingomis atrodančios problemos...“*

L. Oilerio žodžius gerai iliustruoja jo paties darbai.

Po ilgų skaičiavimų, liečiančių draugiškuosius skaičius, Oileris rado daliklių sumos rekurentinę formulę

$$\sigma(A)=\sigma(A-1)+\sigma(A-2)-\sigma(A-5)-\sigma(A-7)+\ldots,$$

kuri tiksliau užrašoma šitaip:

$$\sum_{n=-\infty}^{\infty}(-1)^n\sigma\left(A-\frac{3n^2+n}{2}\right)=0.$$

Šioje sumoje n „perbėga“ visus sveikuosius skaičius, be to, laikoma $\sigma(z)=0$, kai $z<0$, o $\sigma(0)=A$.

Stengdamasis įrodyti savo formulę, Oileris rado kitą, dabar jo vardu vadinamą tapatybę

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{n=-\infty}^{\infty}(-1)^n x^{(3n^2+n)/2},$$

kurią logaritmuojant gaunama ankstesnė formulė. Paskutinės tapatybės dešiniojoje pusėje esanti suma yra vadinamoji *teta funkcija*. Tapatybė šią funkciją susieja su *Dedekindo eta funkcija*. Naudodamasis šiomis iš jų išplaukiančiomis formulėmis, 1972 m. I. G. Makdonaldas atrado daug Dedekindo eta funkcijos tapatybių, susietų su pirminėmis Li G grupėmis. Tos grupės – šiuolaikinės matematikos aktualioji problematika; jų teorinė ir praktinė reikšmė labai didelė.

Šiame paragrafe paminėjome tik kelias aritmetines funkcijas. Pastaruoju metu jos intensyviai tiriamos. Toje srityje sėkmingai dirba ir Lietuvos matematikai. Prof. *J. Kubilius* pirmasis pasaulyje pradėjo sistemingai taikyti tikimybių teorijos metodus aritmetinėms funkcijoms. Susiformavo nauja matematikos šaka – *tikimybinė skaičių teorija*. Be prof. J. Kubiliaus, sėkmingai dirba daug jo mokinių Vilniaus universitete ir Vilniaus pedagoginiame institute.

Uždaviniai

106. Raskite $\tau(150)$, $\tau(250)$, $\tau(440)$, $\tau(1024)$, $\tau(999)$.

107. Raskite $\sigma(45)$, $\sigma(124)$, $\sigma_2(42)$, $\sigma_3(24)$, $\sigma_3(100)$.

108. Įrodykite, kad $\tau(n)<2\sqrt{n}$.

109. Išveskite skaičiaus n daliklių kubų sumos formulę.

110. Raskite didžiausią skaičiaus 7 laipsnį, iš kurio dalijasi 500!.

111. Raskite natūrinį skaičių n, kuris turi tik 2 pirminius daliklius, be to, $\tau(n)=6$, o $\sigma(n)=28$.

112. Kokios turi būti $a \neq 0$ sveikosios reikšmės, kad skaičius ax^2+2x+1 su jokiomis sveikosiomis x reikšmėmis nesidalytų iš 7?

113. Kiek yra tokių sveikų teigiamųjų skaičių x, mažesnių už 10 000, su kuriais 2^x-x^2 nesidalija iš 7?

114. Kokias gauname liekanas dalydami sveikųjų skaičių kubus iš 7?

115. Išspręskite lygtį $\tau(x)+\sigma(x)=16$.

§13. Pirminių skaičių pasiskirstymas

Nagrinėdami pirminių skaičių lenteles, matome, kad imant vis didesnių skaičių intervalus pirminių skaičių procentas mažėja. Štai

intervale	1 – 100	pirminių skaičių yra	25,	t. y.	25%,
„	101 – 200	„	21	„	21%,
„	201 – 300	„	16	„	16%,
„	301 – 400	„	16	„	16%,
„	401 – 500	„	17	„	17%,
„	501 – 600	„	14	„	14%.

Nedidelę išimtį, kaip matome, sudaro penktojo šimto skaičiai. Tūkstančio ilgio intervaluose pirminių skaičių procentas mažėja sparčiau:

intervale	1 – 1000	pirminių skaičių yra	168,	t.y.	17%,
„	1001 – 2000	„	135	„	14%,
„	2001 – 3000	„	127	„	13%,
„	3001 – 4000	„	120	„	12%,
„	4001 – 5000	„	119	„	12%,
„	5001 – 6000	„	114	„	11%.

Iš viso intervale 1 – 10 000 pirminių skaičių yra 1229, t. y. 12%.

Beikerio ir Grunbergerio lentelėse pirminiai skaičiai sudaro 6% visų skaičių.

Galima nurodyti kiek norima daug iš eilės einančių natūrinių skaičių, tarp kurių nėra nė vieno pirminio. Pavyzdžiui, vienas po kito einantys skaičiai

$$k!+2,\ k!+3,\ k!+4,\ \ldots,\ k!+k$$

yra sudėtiniai.

Pirminių skaičių žinoma ne tiek jau daug. Iki 1950 m. didžiausias žinomas pirminis skaičius buvo

$$2^{127}-1=170\ 141\ 183\ 460\ 469\ 231\ 731\ 687\ 303\ 715\ 884\ 105\ 727.$$

Kaip jau minėjome, 1983 m. didžiausias žinomas pirminis skaičius buvo

$$M_{86243}=2^{86243}-1.$$

Atrodytų, kad pirminių skaičių aibė yra baigtinė, tačiau taip nėra. Lengva įrodyti, kad tarp n ir $n!$ (kai $n>2$) yra bent vienas pirminis skaičius. Iš tikrųjų skaičius $m=n!-1$ yra didesnis už 1 ir todėl turi pirminį daliklį p, be to, $p>n$, nes priešingu atveju būtų

$$p \leqslant n \wedge p \mid m \Rightarrow p \mid n! \wedge p \mid m \Rightarrow p \mid (m-n!) \Rightarrow p \mid (-1).$$

Tai prieštarauja pirminio skaičiaus apibrėžimui. Taigi egzistuoja toks pirminis skaičius p, kad

$$n < p \leqslant m < n!.$$

Iš įrodytojo teiginio išplaukia, kad pirminių skaičių aibė yra begalinė. Iš tikrųjų galima sudaryti be galo daug $[n, n!]$ pavidalo nesusikertančių intervalų.

Jau gana seniai žinoma, kad pirminių skaičių aibė begalinė. Senovės graikų matematiko *Euklido* (III a. pr. m. e.) veikaluose randame stebėtinai gražų to teiginio įrodymą.

24 (Euklido) teorema. *Pirminių skaičių aibė yra begalinė.*

Įrodymas. Tarkime, kad ta aibė – baigtinė ir didžiausias pirminis skaičius yra p. Imkime skaičių, vienetu didesnį už visų tų pirminių skaičių sandaugą:

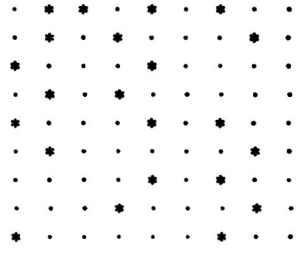
$$N = 2 \cdot 3 \cdot 5 \ldots p + 1.$$

Skaičius $N > 1$ nėra sudėtinis, nes jį dalydami iš bet kurio pirminio gauname liekaną 1. Skaičius $N > p$ nėra ir pirminis, nes didžiausias pirminis pagal prielaidą yra p.

Gautasis prieštaravimas rodo, kad teorema teisinga.

Viena iš sudėtingiausių problemų, susijusių su pirminiais skaičiais, yra jų pasiskirstymas natūrinių skaičių sekoje. Peržvelgus natūrinius skaičius, atrodo, kad pirminiai skaičiai yra išsibarstę be jokios regimos tvarkos.

Pavyzdžiui, jeigu surašytume į kvadratinę lentelę natūrinius skaičius nuo 1 iki 81 (į eilutę rašydami po 9 skaičius), paskui visus pirminius skaičius pažymėtume žvaigždutėmis o kitus – taškais, tai gautume tokį pirminių skaičių išsibarstymo grafinį vaizdą:



Kad ir kiek turėtume taip sužymėtų eilučių, be skaičiavimo nebūtų aišku, kaip sužymėti tolesnę eilutę.

Išsiaiškinsime, kiek yra pirminių skaičių, ne didesnių už realųjį teigiamą skaičių x. Jų skaičių žymime $\pi(x)$, taigi

$$\pi(x) = \sum_{p \leqslant x} 1.$$

Euklido teorema tvirtina, kad pirminių skaičių aibė begalinė. Tą teiginį galime išreikšti lygybe

$$\lim_{x \to \infty} \pi(x) = \infty.$$

Tačiau iš tos teoremos neaišku, kaip iš tikrųjų didėja funkcija $\pi(x)$. Daug matematikų ieškojo formulės, kuria būtų galima išreikšti $\pi(x)$ žinomomis elementariosiomis funkcijomis, tačiau visi tie bandymai buvo nesėkmingi.

1808 m. Ležandras paskelbė apytikslę formulę

$$\pi(x) \approx \frac{x}{\ln x - 1{,}08366}, \tag{1.34}$$

kurią jis nustatė empiriniu būdu (t. y. remdamasis statistiniais duomenimis, lentelėmis spėjo, kad turi būti tokia formulė). Ležandro formulė pasirodė gana tiksli su dideliais x, tačiau matematiškai jos pagrįsti nesisekė. Gausas, kuris jaunystėje taip pat daug laiko skyrė pirminių skaičių vidutiniam tankiui nustatyti, spėjo, kad tikslesnė yra formulė

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}. \tag{1.35}$$

Kadangi

$$\int_2^x \frac{dt}{\ln t} = \frac{x}{\ln x} + \frac{x}{\ln^2 x} + \ldots + \frac{x}{\ln^k x} + \int_2^x \frac{dt}{\ln^{k+1} x} + C,$$

C – tam tikra konstanta, tai nesunku apskaičiuoti, kad iš Gauso (1.35) formulės išplaukia formulė

$$\pi(x) \approx \frac{x}{\ln x - 1},$$

kuri ne tokia tiksli kaip (1.35), bet tikslesnė už (1.34). Kaip vėliau paaiškėjo, Gausas buvo teisus: (1.35) formulė pakankamai tiksliai išreiškia $\pi(x)$. Vėliau kitų matematikų buvo apskaičiuotas skirtumo

$$\pi(x) - \int_2^x \frac{dt}{\ln t}$$

didumas, kuris vis tikslinamas.

Visi tie rezultatai per daug sudėtingi, kad juos būtų įmanoma čia išdėstyti. Kitame paragrafe įrodysime Čebyšovo nelygybę, iš kurios matysime, kad trupmena $\frac{x}{\ln x}$ apytiksliai išreiškia funkcijos $\pi(x)$ didėjimą.

§14. Čebyšovo nelygybė

Tiriant pirminių skaičių pasiskirstymą, pirmąjį rimtą žingsnį pavyko padaryti 1850 m. rusų matematikui *P. Čebyšovui.* Jis įrodė, kad su pakankamai dideliais skaičiais x teisinga nelygybė

$$0{,}89 \frac{x}{\ln x} < \pi(x) < 1{,}11 \frac{x}{\ln x}.$$

Ši nelygybė vadinama Čebyšovo vardu. Vadovėlio I leidime buvo pateiktas toks jos įrodymas, kokį sukūrė Čebyšovas. Jis ilgokas, todėl pateiksime paprastesnį įrodymo variantą su kiek blogesnėmis konstantomis.

Čebyšovo nelygybei įrodyti reikalinga formulė, nurodanti, su kuriuo rodikliu pirminis skaičius p įeina į faktorialo $n!$ kanoninį skaidinį. Beje, ta formulė įdomi ir pati savaime.

25 teorema. *Skaičiaus $n!$ kanoniniame skaidinyje pirminio skaičiaus p laipsnis yra*

$$\alpha=\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]. \tag{1.36}$$

Įrodymas. Taikysime indukcijos metodą. Teoremos tvirtinimas teisingas, kai $n=1$, nes tuo atveju (1.36) formulės dešinioji pusė lygi 0. Tarkime, kad (1.36) formulė teisinga su visais skaičiais $n<m$. Įrodysime, kad ji teisinga ir kai $n=m$.

Sandaugoje

$$m!=1\cdot 2\cdot 3\ldots(m-1)m \tag{1.37}$$

išrenkame tuos dauginamuosius, kurie dalijasi iš p. Visi jie yra skaičiaus p kartotiniai. Kadangi pagal 1 teoremą yra $\left[\frac{m}{p}\right]$ natūrinių skaičių, kurie ne didesni už p ir dalijasi iš p, tai paskutinis (1.37) sandaugos daugiklis – p kartotinis – yra skaičius $\left[\frac{m}{p}\right]p$. Kitų (1.37) sandaugos daugiklių, kurie nėra p kartotiniai, sandaugą žymėsime t:

$$m!=p\cdot 2p\cdot 3p\ldots\left[\frac{m}{p}\right]p\cdot t=p^{\left[\frac{m}{p}\right]}\left[\frac{m}{p}\right]!\,t.$$

Skaičius t tarpusavyje pirminis su p, į jo kanoninį skaidinį p neįeina. Skaičius $\left[\frac{m}{p}\right]<m$ ir todėl pagal indukcijos prielaidą $\left[\frac{m}{p}\right]!$ kanoniniame skaidinyje p rodiklis yra

$$\alpha_1=\sum_{k=1}^{\infty}\left[\frac{\left[\frac{m}{p}\right]}{p^k}\right].$$

Iš paskutinių dviejų lygybių išplaukia, kad skaičiaus $n!$ kanoniniame skaidinyje p rodiklis yra

$$\alpha=\left[\frac{m}{p}\right]+\sum_{k=1}^{\infty}\left[\frac{\left[\frac{m}{p}\right]}{p^k}\right].$$

Remiantis 1 teoremos išvada ((1.4) formulė),

$$\alpha=\left[\frac{m}{p}\right]+\sum_{k=1}^{\infty}\left[\frac{m}{p^{k+1}}\right].$$

Nesunku įsitikinti, kad pastarąją lygybę galima užrašyti šitaip:

$$\alpha = \sum_{k=1}^{\infty} \left[\frac{m}{p^k}\right].$$

Remiantis sustiprintos matematinės indukcijos principu, formulė teisinga su kiekvienu natūriniu skaičiumi n.

Lema. *Tarkime, kad s yra didžiausias rodiklis, su kuriuo pirminis skaičius p įeina į binominio koeficiento C_n^r kanoninį skaidinį. Tada*

$$p^s \leqslant n.$$

Įrodymas. Turime

$$C_n^r = \frac{n(n-1)\cdot\ldots\cdot(n-r+1)}{1\cdot 2\ldots r} = \frac{n!}{r!\cdot(n-r)!}.$$

Pasirėmę 25 teoremos formule, gauname

$$s = \sum_{k=1}^{\infty} \left(\left[\frac{n}{p^k}\right] - \left[\frac{r}{p^k}\right] - \left[\frac{n-r}{p^k}\right]\right).$$

Šios sumos kiekvienas dėmuo lygus 0 arba 1 (tai išplaukia iš (1.3) nelygybės). Dėmenys tikrai lygūs nuliui, kai

$$k > \frac{\ln n}{\ln p}.$$

Taigi

$$s \leqslant \left[\frac{\ln n}{\ln p}\right].$$

Iš pastarosios nelygybės ir išplaukia lemos tvirtinimas.

26 teorema. *Su visais $x>0$ teisinga nelygybė*

$$0{,}66\,\frac{x}{\ln x} < \pi(x) < 1{,}7\,\frac{x}{\ln x}.$$

Įrodymas. Kadangi

$$2^{2n} = (1+1)^{2n} = C_{2n}^0 + C_{2n}^1 + \ldots + C_{2n}^n + \ldots + C_{2n}^{2n},$$

tai

$$C_{2n}^n < 2^{2n}.$$

Kita vertus, kadangi

$$C_{2n}^n = \frac{(2n)!}{(n!)^2} = \frac{2n\cdot(2n-1)\ldots 2\cdot 1}{\left(n\cdot(n-1)\ldots 2\cdot 1\right)^2},$$

tai kiekvienas pirminis skaičius, didesnis už n ir mažesnis už $2n$, gali įeiti tik į skaitiklio kanoninį skaidinį. Todėl C_{2n}^{n} dalijasi iš kiekvieno pirminio skaičiaus p, esančio tarp n ir $2n$. Taigi

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leqslant 2n} p < C_{2n}^{n} < 2^{2n}.$$

Logaritmuodami šią nelygybę, gauname

$$\pi(2n)-\pi(n) < \frac{2n\cdot \ln 2}{\ln n} < 1{,}39\ \frac{n}{\ln n}.$$

Teoremos dešiniosios nelygybės įrodymą užbaigsime matematinės indukcijos metodu.

Tiesiogiai skaičiuojant, galima įsitikinti, kad teoremos tvirtinimas teisingas, kai $x<1200$. Todėl laikysime $x\geqslant 1200$. Pagal indukcijos prielaidą

$$\pi(n) < 1{,}7\ \frac{n}{\ln n}.$$

Sudėję dvi paskutines nelygybes, gauname

$$\pi(2n) < 3{,}09\ \frac{n}{\ln n} < 1{,}7\ \frac{2n}{\ln 2n}.$$

Kadangi, kai $n\geqslant 1200$,

$$\pi(2n+1)\leqslant \pi(2n)+1 < 3{,}09\ \frac{n}{\ln n}+1 < 1{,}7\ \frac{2n+1}{\ln(2n+1)},$$

tai teoremos dešinioji nelygybė teisinga su visais natūriniais skaičiais x.

Teoremos kairiąją nelygybę įrodysime remdamiesi lema. Pažymėję s_p rodiklį, su kuriuo pirminis skaičius p įeina į C_n^r, ir pasirėmę lemos nelygybe, gauname

$$C_n^r = \prod_{p\leqslant n} p^{s_p} \leqslant n^{\pi(n)}.$$

Kadangi pastaroji nelygybė teisinga su visais r, $0\leqslant r\leqslant n$, tai

$$2^n = (1+1)^n = \sum_{r=0}^{n} C_n^r < (n+1)\,n^{\pi(n)}.$$

Išlogaritmavę tą nelygybę ir pasirėmę sąlyga $n\geqslant 1200$, galime gauti

$$\pi(n) > \frac{n\cdot \ln 2}{\ln n} - \frac{\ln(n+1)}{\ln n} > 0{,}66\ \frac{n}{\ln n}.$$

Iš Čebyšovo nelygybės išplaukia n-ojo pirminio skaičiaus įverčiai.

Čebyšovo nelygybę galime užrašyti šitaip:

$$a\frac{n}{\ln n} < \pi(n) < A\frac{n}{\ln n}; \qquad (1.38)$$

čia a ir A – teigiamos konstantos ir $a<1<A$. Kuo tikslesniais metodais įrodinėjama Čebyšovo tipo nelygybė, tuo mažiau tos konstantos skiriasi nuo 1.

Pažymėsime p_n n-ąjį iš eilės pirminį skaičių: $p_1=2$, $p_2=3$ ir t. t.

27 teorema. *Egzistuoja tokios dvi konstantos b ir B, $0<b<B$, kad su visais pirminiais skaičiais p_n $(n>2)$ teisingos nelygybės*

$$bn\ln n<p_n<Bn\ln n. \tag{1.39}$$

Įrodymas. Iš Čebyšovo (1.38) nelygybės išplaukia

$$a\frac{p_n}{\ln p_n}<\pi(p_n)<A\frac{p_n}{\ln p_n}.$$

Remiantis funkcijos $\pi(x)$ apibrėžimu, $\pi(p_n)=n$. Todėl iš pastarosios nelygybės gauname

$$p_n<\frac{1}{a}n\ln p_n, \tag{1.40}$$

$$p_n>\frac{1}{A}n\ln p_n\geqslant\frac{1}{A}n\ln n,$$

nes akivaizdu, kad $p_n>n$.

Pažymėję $b=A^{-1}$, gauname kairiąją (1.39) nelygybės pusę. Tos nelygybės dešiniosios pusės įrodymą baigsime pastebėję, kad $\ln p_n<\sqrt{p_n}$, kai p_n pakankamai didelis. Tuomet iš šios bei (1.40) nelygybių išplaukia

$$p_n<\frac{1}{a}n\sqrt{p_n},$$

$$p_n<a^{-2}n^2,$$

$$\ln p_n<-2\ln a+2\ln n<c\ln n;$$

čia c – tam tikra konstanta. Lieka pažymėti $B=c\cdot a^{-1}$.

Vadinasi, (1.39) nelygybė teisinga, kai n pakankamai didelis skaičius. Šia sąlyga buvo remtasi įrodinėjant dešiniąją nelygybę. Konstantą B pakeitus atitinkamai didesne, teorema būtų teisinga su bet kuriuo pirminiu skaičiumi.

28 teorema. *Eilutė, sudaryta iš pirminiams skaičiams atvirkštinių skaičių, diverguoja.*

Įrodymas. Pasirėmę nelygybe $p_n<Bn\ln n$, turime

$$\sum_{n=2}^{\infty}\frac{1}{p_n}>\sum_{n=2}^{\infty}\frac{1}{Bn\ln n}.$$

Tačiau

$$\frac{1}{n\ln n}>\int_n^{n+1}\frac{dx}{x\ln x},$$

nes pointegralinė funkcija mažėja intervale $[n, n+1]$, jos didžiausia reikšmė yra $\frac{1}{n\ln n}$. Iš tos nelygybės gauname

$$\sum_{n=1}^{\infty}\frac{1}{p_n}=\frac{1}{2}+\sum_{n=2}^{\infty}\frac{1}{p_n}>\frac{1}{2}+\sum_{n=2}^{\infty}\frac{1}{b}\int_{n}^{n+1}\frac{dx}{x\ln x}=\frac{1}{2}+\frac{1}{b}\int_{2}^{\infty}\frac{dx}{x\ln x}.$$

Pastarasis integralas diverguoja, nes

$$\int\frac{dx}{x\ln x}=\ln\ln x.$$

Teorema įrodyta.

Atkreipsime dėmesį, kad eilutė, sudaryta iš skaičių, atvirkštinių natūrinių skaičių kvadratams, konverguoja:

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\zeta(2)=\frac{\pi^2}{6}.$$

Taigi pirminių skaičių aibė žymiai tankesnė už natūrinių skaičių kvadratų aibę.

Uždaviniai

116. Įrodykite, kad n-asis pirminis skaičius $p_n>2n$ $(n>4)$.

117. Raskite, kurie 3 laipsniai įeina į šių skaičių kanoninius skaidinius: a) 300!; b) 621!; c) 1200!.

118. Remdamiesi Čebyšovo nelygybe bei jo gautais konstantų įvertčiais, nurodykite funkcijos $\pi(x)$ apatinius ir viršutinius rėžius, kai: a) $x=10!$; b) $x=10^{30}$; c) $x=2^{100}$.

119. Remdamiesi Čebyšovo nelygybe, raskite intervalus, kuriuose yra n-asis pirminis skaičius, kai: a) $n=100^{10}$; b) $n=10^{30}$; c) $n=2^{60}$.

120. Raskite bent vieną nelygybės $p_{10000}<x$ sprendinį (čia p_n – n-asis pirminis skaičius).

§15. Pirminių skaičių asimptotinis pasiskirstymas

Taikydami itin sudėtingus skaičių teorijos metodus, galime įrodyti, kad su pakankamai dideliais x konstantos a ir A nuo 1 skiriasi kiek norima mažai, t. y. Gauso (1.35) formulė yra tiksli ir

$$\lim_{x\to\infty}\frac{\pi(x)}{\int_{2}^{x}\frac{dt}{\ln t}}=\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1. \tag{1.41}$$

1886 m. prancūzų matematikas *Ž. Adamaras* (J. Hadamard, 1865–1963) ir belgų matematikas *Š. Valė Pusenas* (Ch. de la Vallée Poussin, 1866–1962), nepriklausomai vienas nuo kito, įrodė (1.41) ribinį dėsnį, t. y. kai x pakankamai didelis, funkciją $\pi(x)$ tinkamai aproksimuoja ir santykis $\frac{x}{\ln x}$,

ir integralinis logaritmas $\operatorname{li} x = \int_2^x \frac{dt}{\ln t}$. Pateikiamoje lentelėje matome, kaip didėjant x kinta $\pi(x)$ ir integralinio logaritmo santykis.

x	$\pi(x)$	$\operatorname{li} x$	$\pi(x)/\operatorname{li} x$
1000	168	235	0,94
10000	1229	1246	0,98
100000	9592	9630	0,996
1000000	78498	78628	0,9983
10000000	664579	664918	0,9994
100000000	5761455	5762209	0,99986
1000000000	50847478	50849235	0,99996

Matome, kad li x reikšmės didesnės už funkcijos $\pi(x)$ reikšmes. Tačiau taip yra ne visada.

Neretai būna, kad ir labai išsamūs statistiniai skaičiavimai ne visai tiksliai atspindi tikrąją padėtį. Štai, nagrinėjant pirminius skaičius, ne didesnius už 1 milijoną, susidaro įspūdis, kad 13 paragrafe pateikta Ležandro formulė tikslesnė už Gauso formulę – integralinį logaritmą. Tačiau, pradedant maždaug nuo $x = 5\,000\,000$, integralinis logaritmas li x žymiai tiksliau apibūdina $\pi(x)$ negu Ležandro formulė.

Nagrinėjant klausimą, kaip tiksliai li x išreiškia pirminių skaičių, ne didesnių už x, kiekį, buvo tiriamas skirtumo li $x - \pi(x)$ didumas. Pažymėkime tą skirtumą $s(x)$:

$$s(x) = \operatorname{li} x - \pi(x).$$

Išsamūs statistiniai skaičiavimai, atlikti gana dideliame intervale, rodo, kad skirtumas $s(x)$ yra teigiamas. Atrodytų, kad jis turi tendenciją augti iki begalybės. Net iki $x = 10^9$ li x reikšmės didesnės už $\pi(x)$ reikšmes. Tačiau iš tikrųjų $s(x)$ ne visuomet teigiamas.

Anglų matematikas *J. E. Litlvudas* (J. E. Littlewood) įrodė, kad egzistuoja tokios x reikšmės, su kuriomis $s(x) < 0$. Tiesa, iki šiol nerasta nė vienos konkrečios tokios x reikšmės. Dargi nelabai tikima, kad apskritai kada nors pavyks tokių reikšmių rasti, nes jos turėtų būti labai didelės. Kitas anglų matematikas *S. Skjūzas* (S. Skews) 1933 m., laikydamas teisinga vadinamąją *Rymano hipotezę* (apie ją kiek vėliau kalbėsime), įrodė, kad bent viena x reikšmė, su kuria $s(x) < 0$, ne didesnė už skaičių

$$10^{10^{10^{34}}}.$$

Po 22 metų tas pats Skjūzas, jau nebesiremdamas Rymano hipoteze, įrodė, kad yra tokia x reikšmė, ne didesnė už

$$10^{10^{10^{964}}},$$

su kuria $\pi(x) > \operatorname{li} x$. Šis antrasis rėžis didesnis už pirmąjį, tačiau jis visiškai tikslus, neparemtas jokiomis hipotezėmis. Tie rezultatai vėliau buvo dar patikslinti. 1966 m. *E. Lemanas* (E. Lehman) įrodė, kad tarp skaičių $1{,}53 \cdot 10^{1165}$ ir $1{,}65 \cdot 10^{1165}$ yra intervalas, turintis ne mažiau kaip 10^{500} skaičių. Tame intervale yra toks x_0, su kuriuo $s(x_0) < 0$. Remiantis Lemano rezultatais, tikėtina, kad su jokiu x, mažesniu už 10^{20}, $s(x)$ negali būti neigiamas.

Adamaras ir Valė Pusenas, įrodydami (1.41) dėsnį, rėmėsi *B. Rymano* (B. Riemann, 1826–1866, vokiečių matematikas ir fizikas) idėja, kad funkcijos $\pi(x)$ didėjimo dėsnis susijęs su funkcijos

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

vadinamos *Rymano dzeta funkcija*, analizinėmis savybėmis. $\zeta(s)$ yra kompleksinio kintamojo $s = \sigma + it$ funkcija srityje $\sigma > 1$. Jeigu $\sigma \leqslant 1$, tai eilutė diverguoja. Tuo atveju funkcija $\zeta(s)$ apibrėžiama kitomis eilutėmis. $\zeta(s)$ ir $\zeta(1-s)$ sąryšis vadinamas Rymano dzeta funkcijos *funkcionaline* lygtimi, kuria remiantis ta funkcija apibrėžiama beveik visoje kompleksinio kintamojo s plokštumoje. Kaip Rymano dzeta funkcija susijusi su pirminiais skaičiais, matome iš *Oilerio tapatybės*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-1/p^s} (\sigma > 1);$$

čia dauginama pagal visus pirminius skaičius.

Įrodyta, kad $\zeta(s)$ turi be galo daug nulių. Visi kompleksiniai nuliai yra juostoje

$$0 < \sigma < 1,$$

o realieji nuliai – neigiamoje realiosios ašies atkarpoje. Pasirodo, kad arti tiesės $\sigma = 1$ $\zeta(s)$ nulių nėra. Kuo toliau nuliai nuo tos tiesės, tuo tikslesnis skirtumo $\pi(x) - \operatorname{li} x$ įvertinimas. Įrodyta (*I. Vinogradovas* ir *N. Korobovas*), kad $\zeta(s)$ nulių nėra srityje

$$\sigma > 1 - \frac{c(\alpha)}{\log^{\alpha} t};$$

čia $\alpha > \frac{2}{3}$, $c(\alpha)$ – konstanta. Iš to išplaukia šitoks pirminių skaičių pasiskirstymo dėsnis:

$$\left| \pi(x) - \int_2^x \frac{dt}{\ln t} \right| < Cxe^{-a(\ln x)^{3/5-\varepsilon}};$$

čia $a > 0$, $\varepsilon > 0$, $C > 0$ – konstantos.

B. Rymanas iškėlė hipotezę, kad visi kompleksiniai dzeta funkcijos $\zeta(s)$ nuliai yra tiesėje

$$\sigma = \frac{1}{2}.$$

Tai viena iš sudėtingiausių ir viena iš pagrindinių skaičių teorijos problemų. Įrodžius tą hipotezę, būtų galima įrodyti daug įvairių skaičių teorijos teiginių. Iš Rymano hipotezės teisingumo išplauktų toks pirminių skaičių dėsnis:

$$\left| \pi(x) - \int_2^x \frac{dt}{\ln t} \right| \leqslant c\sqrt{x}\ln x.$$

Pastaroji nelygybė žymiai tikslesnė negu prieš ją parašytoji.

Skaičių teorijoje tiriamos ir kitokios aibės. Nagrinėjami racionaliųjų skaičių aibės Q plėtiniai, vadinamieji *algebrinių skaičių laukai*, apibrėžiami tų laukų „sveikieji" ar „pirminiai" skaičiai, tiriami tų skaičių pasiskirstymo dėsningumai. Sudaromos Rymano dzeta funkcijai analogiškos funkcijos, kurioms galima formuluoti hipotezes, analogiškas Rymano hipotezei. Viena iš tokių funkcijų yra vadinamoji *Hekės dzeta funkcija*, kuri nuo Rymano dzeta funkcijos skiriasi tuo, kad atitinkamos trupmenos skaitiklyje yra ne 1, o dydis, lygus 0 arba vienetinio modulio kompleksiniam skaičiui — *Hekės charakteriui* (E. Hecke, 1887—1947, vokiečių matematikas).

Hekės dzeta funkcijos minėtinos dar ir dėl to, kad jų teoriją plėtojo ir Lietuvos matematikai. Prof. J. Kubilius, remdamasis savo rezultatais apie Hekės dzeta funkcijas ir pirminių algebrinių skaičių pasiskirstymą, įrodė šitokį *E. Landau* (1877—1938) hipotezės variantą: egzistuoja be galo daug pirminių skaičių p, užrašomų suma

$$p = a^2 + b^2,$$

kurioje dėmuo b^2 pakankamai mažas, lyginant su dėmeniu a. Pati Landau hipotezė šitokia: yra be galo daug

$$p = a^2 + 1$$

pavidalo pirminių skaičių.

Įdomūs ir kiti prof. J. Kubiliaus ir jo mokinių gauti rezultatai. Matematikos mokytojai turėtų skatinti moksleivių kūrybiškumą, domėjimąsi matematikos problemomis, ypač tomis, kurios nagrinėjamos Lietuvoje.

Šiame paragrafe pateiktos nelygybės bei kitos formulės teikia tam tikros informacijos apie funkcijos $\pi(x)$ kitimą, kai x pakankamai didelis skaičius. Kintamajam x neribotai didėjant, santykinė įverčių paklaida mažėja, todėl šio tipo pirminių skaičių pasiskirstymo dėsniai vadinami *asimptotiniais* (t. y. tuo tikslesniais, kuo x didesnis).

§16. Pirminiai skaičiai aritmetinėse progresijose

Kartu su pirminių skaičių pasiskirstymu natūrinių skaičių sekoje buvo tiriamas ir pirminių skaičių tankis aritmetinėse progresijose

$$a,\ a+m,\ a+2m,\ a+3m,\ \ldots$$

Aišku, jeigu $(a, m)>1$, tai visi tokios progresijos nariai (išskyrus nebent pirmąjį) yra sudėtiniai skaičiai. Taigi pirminiai skaičiai gali būti tik tokiose progresijose, kurių pirmasis narys ir progresijos skirtumas yra tarpusavyje pirminiai skaičiai. 1837 m. vokiečių matematikas *Dirichlė* (P. G. Lejeune-Dirichlet, 1805–1859) įrodė, kad aritmetinėje progresijoje $a+mt$ ($t\in\mathbb{N}$) yra be galo daug pirminių skaičių, kai $(a, m)=1$. Tas teiginys vadinamas *Dirichlė teorema.*

Jau minėjome, kad yra $\varphi(m)$ natūrinių skaičių, ne didesnių už m ir tarpusavyje pirminių su m ($\varphi(m)$ – Oilerio funkcija). Taigi ir aritmetinių progresijų, kurių skirtumas m ir kurios turi be galo daug pirminių skaičių, taip pat yra $\varphi(m)$.

Pasirodo, kad visi pirminiai skaičiai yra tolygiai pasiskirstę po tas progresijas, t. y. kiekvienoje iš tų progresijų yra toks pat asimptotinis pirminių skaičių tankis. Jeigu simboliu

$$\pi_a(m, x)$$

žymėsime skaičių pirminių skaičių, priklausančių progresijai $a+mt$ ir ne didesnių už x, tai

$$\pi_a(m, x) \sim \frac{1}{\varphi(m)} \int_2^x \frac{dt}{\ln t},$$

kai $(a, m)=1$.

Tą teiginį įrodė *Valė Pusenas.* Jis gavo formulę

$$\pi_a(m, x)=\frac{1}{\varphi(m)} \int_2^x \frac{dt}{\ln t}+c_1 x e^{-c_2\sqrt{\ln x}},$$

kurioje c_1 ir c_2, $c_2>0$, – konstantos.

Pirminių skaičių pasiskirstymo aritmetinėse progresijose dėsnis tikslinamas ir dabar, taikomi sudėtingi analiziniai metodai, paremti vadinamųjų *Dirichlė eilučių*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

(čia $\chi(n)$ reiškia tam tikrą *Dirichlė charakteriu* vadinamą kompleksinį skaičių, kurio modulis yra 0 arba 1; $s=\sigma+it$ – kompleksinis kintamasis) nulių savybėmis.

Dirichlė teoremos įrodymas gana sudėtingas, čia jo nepateiksime. Atskiri šios teoremos atvejai gali būti įrodyti elementariai. Išnagrinėsime aritmetines progresijas su skirtumais 4 ir 6.

Yra 4 aritmetinės progresijos su skirtumu 4, atitinkančios 4 a reikšmes: $4t, 1+4t, 2+4t, 3+4t$. Akivaizdu, kad pirminių skaičių gali būti tik progresijose $1+4t$ ir $3+4t$ ($t\in\mathbb{N}$). Su skirtumu 6 taip pat yra tik dvi progresijos $1+6t$ ir $5+6t$, kuriose be galo daug pirminių skaičių. Progresijas $1+4t$ ir $1+6t$ nagrinėsime IV skyriuje – reikalingi kai kurie dėsniai, kurių dar nenagrinėjome. Progresijas $3+4t$ ir $5+6t$ aptarsime dabar. Beje, patogiau jas nagrinėti nžrašius atitinkamai $-1+4t$ ir $-1+6t$ pavidalu.

29 teorema. *Yra be galo daug* $-1+4t$ *bei* $-1+6t$ *pavidalo pirminių skaičių.*

Įrodymas. Įrodysime teiginį apie $-1+4t$ pavidalo pirminius skaičius. Tarkime, kad tokių skaičių yra baigtinis skaičius. Pažymėję jų sandaugą M, nagrinėkime, iš kokių pirminių skaičių galima padalyti skaičių $4M-1$.

Jau minėjome, kad visi pirminiai skaičiai skirstomi į dvi grupes (progresijas skirtumo 4 atžvilgiu): jie yra arba $4t+1$, arba $4t-1$ pavidalo. Tačiau bet kurių dviejų $4t+1$ pavidalo skaičių sandauga vėl $4t+1$ pavidalo skaičius:

$$(4t_1+1)(4t_2+1)=16t_1t_2+4t_1+4t_2+1=4t_3+1.$$

Skaičius $4M-1$ nėra $4t+1$ pavidalo, todėl jis turi turėti bent vieną pirminį $4t-1$ pavidalo daliklį p. Priminsime, kad visų tokių pirminių skaičių sandauga pagal prielaidą pažymėta M. Bet iš sąryšių

$$p \mid 4M-1 \quad \text{ir} \quad p \mid M$$

išplaukia $p \mid -1$. Tai prieštarauja pirminio skaičiaus apibrėžimui. Šio prieštaravimo priežastis – prielaida, kad $4t-1$ pavidalo pirminių skaičių aibė baigtinė. Taigi tokių pirminių skaičių yra be galo daug.

Analogiškai įrodomas ir teoremos teiginys, kad yra be galo daug $6t-1$ pavidalo pirminių skaičių.

Dirichlė teorema nenurodo pirmojo progresijos pirminio skaičiaus, kuris gali būti labai didelis. Šiuo požiūriu labai įdomų rezultatą gavo tarybinis matematikas *J. Linikas* (1915–1973). Jis įrodė šitokią teoremą.

Liniko teorema. *Egzistuoja tokia konstanta* c, *kad mažiausias pirminis progresijos*

$$a,\ a+m,\ a+2m,\ \ldots$$

skaičius, kai $(a, m)=1$, *yra ne didesnis už* m^c.

Teoremos įrodymas sudėtingas ir čia jo nepateiksime.

Trumpai paminėsime kai kuriuos paskirus rezultatus, susijusius su pirminiais skaičiais.

Pažymėkime $\pi_{a,b}(x)$ pirminių skaičių, priklausančių progresijai $b+at$ ir ne didesnių už x, skaičių. Taip pat pažymėkime

$$\Delta(x)=\pi_{4,3}(x)-\pi_{4,1}(x).$$

Skirtumas $\Delta(x)$ yra teigiamas ir nelabai didelis, kai x nedidelis. Pavyzdžiui, $\pi_{4,3}(10^{10})=227\ 529\ 235$, $\pi_{4,1}(10^{10})=227\ 523\ 275$ ir $\Delta=5960$. Pagal Beizo ir Hadzono skaičiavimus $\Delta(x)>0$ iki $x=950\ 000\ 000$, išskyrus mažiau kaip 1000 x reikšmių. Tačiau dar prieš $x=2\cdot 10^{10}$ yra ilgas intervalas $[1, 854\cdot 10^{10}, 1, 895\cdot 10^{10}]$, kuriame $\Delta(x)<0$ ir $\min\Delta(x)=-2719$.

Merseno pirminiai skaičiai dažnai pasitaiko įvairiuose uždaviniuose. Pavyzdžiui, skleisdami laipsnine eilute dydį, atvirkščią kvadratiniam polinomui, kurio šaknys 0,5 ir 1, gauname skleidinį, kurio koeficientai prie x^{n-1} yra Merseno skaičiai M_n:

$$\frac{1}{(1-x)(1-2x)}=M_1+M_2x+M_3x^2+\ldots$$

Formulė apibrėžta, kai $|x|<0{,}5$.

Matematikus domino ne tik 2^n-1, bet ir 2^n+1 pavidalo skaičiai. Jeigu n turi bent vieną nelyginį pirminį daliklį d, tai skaičius 2^n+1 yra sudėtinis (dalijasi iš $2^{n/d}+1$). Taigi 2^n+1 pavidalo skaičiai yra pirminiai, kai $n=2^k$. Garsusis XVII a. prancūzų matematikas *P. Ferma* (P. Fermat, 1601–1665) nustatė, kad skaičiai $2^{2^k}+1$ yra pirminiai, kai $k=0, 1, 2, 3, 4$ (jie atitinkamai lygūs 3, 5, 17, 257, 65 537). Jam kilo mintis, kad visi to pavidalo skaičiai yra pirminiai. Vėliau skaičiai $F_k=2^{2^k}+1$ buvo pavadinti *Ferma skaičiais.*

1732 m. L. Oileris patikrino atvejį, kai $k=5$, ir nustatė, kad skaičius $F_5=2^{2^5}+1$ yra sudėtinis: $F_5=4\ 294\ 967\ 297=641\cdot 6\ 700\ 417$. Tuo minėtoji Ferma hipotezė buvo paneigta.

Apie Ferma skaičius žinoma ne daugiau kaip apie Merseno pirminius skaičius. Šiuo metu žinomi 46 sudėtiniai Ferma skaičiai, iš kurių mažiausias yra F_5, o didžiausias – F_{1945}. Pirminių Ferma skaičių, be tų, kuriuos rado pats Ferma, daugiau nežinoma. Mažiausias iš Ferma skaičių, dar nepriskirtas nei prie pirminių, nei prie sudėtinių, yra F_{17}.

Ferma skaičiai, kaip ir Merseno skaičiai, nėra „izoliuoti“ nuo kitų algebros klausimų. Žymus vokiečių matematikas *K. Gausas* (K. Gauss, 1777–1855) nustatė, kad taisyklingąjį n-kampį galima nubrėžti skriestuvu ir liniuote tik tada, kai n yra pirminis Ferma skaičius arba skiriasi nuo tokio skaičiaus daugikliu 2^α (α – natūrinis). Getingeno (VFR) universiteto rankraštyne saugomas 80 puslapių Hermeso darbas, skirtas taisyklingojo 65 537-kampio brėžimui skriestuvu ir liniuote ($65\ 537=F_4$).

§17. Kitos skaičių teorijos problemos

Plačiau aptarsime *Goldbacho, Varingo* bei *pirminių skaičių – dvynių problemas.*

Goldbacho problema. 1742 m. Peterburgo akademikas *Christijanas Goldbachas* (1690–1764) laiške savo kolegai akademikui Leonardui Oileriui išreiškė spėjimą, kad *bet kurį nelyginį skaičių, didesnį už 5, galima išreikšti trijų pirminių skaičių suma.*

Pavyzdžiui,

$$7=2+2+3,$$
$$9=3+3+3,$$
$$11=3+3+5$$

ir t. t. Toks išreiškimas gali būti nevienareikšmis.

L. Oileris atsakomajame laiške iškėlė hipotezę, kad *bet kurį lyginį skaičių, didesnį už 2, galima išreikšti dviejų pirminių skaičių suma.*

Pavyzdžiui,

$$8=3+5,$$
$$10=5+5,$$
$$12=5+7$$

ir t. t.

Tos problemos buvo pavadintos Goldbacho problemomis: pirmoji – *Goldbacho ternare problema*, antroji – *Goldbacho binare problema*. Jos taip pat vadinamos *Goldbacho ir Oilerio problemomis*.

Akivaizdu, kad iš Goldbacho binarės problemos išplaukia ternarė problema: jeigu $N=2k+1$, tai $N-3$ yra lyginis skaičius ir jį išreiškę dviejų pirminių p ir q suma gautume

$$N=3+p+q.$$

Nors tos problemos atrodo gana paprastos, tačiau beveik per 200 metų nė vienam matematikui nepavyko jų įrodyti. 1912 m. žymus vokiečių matematikas *E. Landau* pasiūlė įrodyti žymiai susilpnintą Goldbacho problemos variantą: bet kurį natūrinį skaičių $N>1$ galima išreikšti k pirminių skaičių suma, kai k gali būti ir gana didelis, bet baigtinis skaičius. Tą hipotezę 1930 m. įrodė tarybinis matematikas *L. Šnirelmanas* (1905–1935).

1934 m. buvo žengtas dar vienas žingsnis. Tarybinis matematikas akademikas *I. Vinogradovas* (1891–1983) sukūrė trigonometrinių sumų metodą, kurį taikydamas įrodė teiginį: *egzistuoja toks natūrinis skaičius* N_0, *kad bet kuris nelyginis skaičius* N, *didesnis už* N_0, *gali būti išreikštas trijų pirminių skaičių suma.*

I. Vinogradovas kartu įrodė, kad nelyginis skaičius N ($N>N_0$) gali būti išreikštas trijų pirminių skaičių suma $I(N)$ būdų, o skaičiui $I(N)$ teisinga asimptotinė formulė (kai $N\to\infty$):

$$I(N)\sim\frac{N^2}{2\ln^3 N}\prod_p\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid N}\left(1-\frac{1}{p^2-3p+3}\right).$$

Taigi ternarė Goldbacho problema iš esmės išspręsta. Lieka įsitikinti, kad ir visi nelyginiai skaičiai N,

$$7\leqslant N\leqslant N_0,$$

išreiškiami trijų pirminių skaičių suma. Deja, to patikrinti dar neįmanoma, nes skaičius N_0 I. Vinogradovo teoremoje gana didelis. Apskaičiuota, kad

$$N_0=e^{e^{16,038}}.$$

Tas skaičius turi daugiau kaip 4,5 milijono skaitmenų.

Binarė Goldbacho problema dar neišspręsta, nors ir nerasta nė vieno jai prieštaraujančio pavyzdžio.

1948 m. vengrų matematikas *A. Rėnis* įrodė, kad kiekvieną pakankamai didelį lyginį skaičių N galima išreikšti šitaip:

$$N=p+n;$$

čia p – pirminis, o n turi ne daugiau kaip k pirminių daugiklių. 1964 m. *A. Buchštabas* įrodė, kad $k\leqslant 3$. Binarė Goldbacho problema būtų išspręsta įrodžius, kad $k=1$.

Varingo problema. 1770 m. anglų matematikas *E. Varingas* (E. Waring, 1734–1798) be įrodymo suformulavo keletą teiginių, kurie vėliau buvo sujungti į vieną problemą, vadinamą jo vardu. 1909 m. Varingo problemą išsprendė žymus vokiečių matematikas *D. Hilbertas* (D. Hilbert, 1862–1943). Jis įrodė šią teoremą.

Imant bet kurį natūrinį skaičių n, galima rasti tokį natūrinį skaičių s, priklausantį nuo n, s=s (n), kad bet koks natūrinis N būtų išreiškiamas s sveikųjų neneigiamų skaičių n-ųjų laipsnių suma:

$$N=x_1^n+x_2^n+\ldots+x_s^n.$$

1770 m. Lagranžas įrodė, kad bet kurį natūrinį skaičių galima išreikšti 4 kvadratų suma.

Pavyzdžiui,

$$10=2^2+2^2+1^2+1^2,$$

$$30=5^2+2^2+1^2+0^2,$$

$$70=8^2+2^2+1^2+1^2$$

ir t. t. Vadinasi,

$$s(2)=4.$$

Įrodyta, kad visus skaičius, išskyrus 23 ir 239, galima išreikšti 8 kubų suma. Tuos du skaičius galima išreikšti tik 9 kubų suma. Vadinasi,

$$s(3)=9.$$

Funkcijos $s=s(n)$ tikroji išraiška dar nenustatyta.

Įrodyta, kad $s(6)=73$, $s(7)=143$, $s(8)=279$. $s(4)$ ir $s(5)$ reikšmės ir dabar nežinomos, tik įrodyta, kad

$$19\leqslant s(4)\leqslant 35.$$

$$37\leqslant s(5)\leqslant 40.$$

Taip pat įrodyta, kad su visais natūriniais n

$$s(n)\geqslant 2^n+\left[\frac{3^n}{2^n}\right]-2. \tag{1.42}$$

Jeigu

$$3^n-2^n\left[\frac{3^n}{2^n}\right]\leqslant 2^n-\left[\frac{3^n}{2^n}\right],$$

tai (1.42) formulėje nelygybės ženklą galima pakeisti lygybės ženklu. 1964 m. *Stemleris*, naudodamasis elektroninėmis skaičiavimo mašinomis, nustatė, kad formulė

$$s(n)=2^n+\left[\frac{3^n}{2^n}\right]-2$$

teisinga su visais natūriniais skaičiais $n\leqslant 200\ 000$.

Pirminių skaičių – dvynių problema. Dvyniais vadinami tokie du pirminiai skaičiai, kurie skiriasi 2. Tokie yra, pavyzdžiui, pirminiai skaičiai 3 ir 5, 5 ir 7, 11 ir 13. Didėjant pirminiams skaičiams dvynių porų skaičius santykinai mažėja. Jeigu iki 100 000 galime suskaičiuoti 1225 dvynių poras, tai intervale nuo 8 000 000 iki 8 100 000 jų yra tik 518. Skaičių dvynių mažėjimą galima iliustruoti statistine lentele, kurioje visi intervalai yra 150 000 vienetų ilgumo.

Kyla klausimas, ar pirminių skaičių – dvynių aibė baigtinė, ar begalinė? Deja, į šį, kaip ir į kiek bendresnį klausimą – ar visuomet išsprendžiama pir-

miniais skaičiais x ir y tiesinė lygtis $ax+by=c$ su sveikaisiais koeficientais ir tarpusavyje pirminiais a ir b, dar vis neatsakyta. (Beje, pastarasis klausimas yra viena iš jau minėtų Hilberto problemų.)

Intervalo pradžia	Pirminių skaičius	Dvynių porų skaičius
10^8	8154	601
10^9	7242	466
10^{10}	6511	389
10^{11}	5974	276
10^{12}	5433	276
10^{13}	5065	208
10^{14}	4643	186
10^{15}	4251	161

Tiriant pirminių skaičių – dvynių problemą, gauta daug įdomių rezultatų. Paminėsime norvegų matematiko *Vigo Bruno* suformuluotą teoremą: *eilutė, sudaryta iš skaičių, atvirkštinių pirminiams dvyniams, konverguoja.* Taigi, jei dvynių aibė ir yra begalinė, ji vis tik žymiai retesnė negu visų pirminių skaičių aibė (palyginkite su 28 teorema).

Viena iš didesnių dvynių porų yra ši: 10 016 957 ir 10 016 959.

Kitos pirminių skaičių problemos. Paminėsime dalį neišspręstų pirminių skaičių problemų (beje, kai kurios iš jų galbūt šiuo metu jau išspręstos ar baigiamos spręsti).

1. Nežinomas nė vienas pirminis skaičius, turintis 1000 skaitmenų, nors žinoma, kad yra mažiausiai 3 tokie skaičiai.
2. Nežinoma, begalinis ar baigtinis yra pirminių skaičių – dvynių skaičius.
3. Neaišku, ar galima įrodyti, kad kiekvienas lyginis skaičius išreiškiamas dviejų pirminių skaičių skirtumu.
4. Nežinoma, ar teisinga Hardy ir Litlvudo hipotezė, kad kiekvienas pakankamai didelis natūrinis skaičius lygus natūrinio skaičiaus kvadrato ir pirminio skaičiaus sumai.
5. Neįrodyta Hilbraito hipotezė (1958 m.): jeigu pirmojoje eilutėje surašysime visus pirminius skaičius, antrojoje eilutėje – gretimų pirminių skaičių skirtumus, trečiojoje – gretimų antrosios eilutės skaičių skirtumus ir t. t., tai kiekviena eilutė prasidės vienetu. Patikrinta, kad ta hipotezė teisinga pirmosioms 63 418 eilučių.
6. Neaišku, kiek yra pirminių skaičių, kurie išlieka pirminiais bet kaip sukeitus jų skaitmenis (pvz., 13 ir 31, 199, 919, 991).
7. Nežinoma, baigtinis ar begalinis yra skaičius pirminių skaičių, kurių pirmasis ir paskutinis skaitmuo 1, o kiti nuliai (pvz. 101).
8. Neaišku, ar su visais natūriniais $x>1$ ir $y>1$ teisinga nelygybė

$$\pi(x+y)\leqslant\pi(x)+\pi(y).$$

9. Neįrodyta, kiek yra p, $p+2$, $p+6$, $p+8$ pavidalo pirminių skaičių ketvertų (pvz., 5, 7, 11, 13). Didžiausias žinomas pirminių skaičių ketvertas gaunamas, kai $p=2\,863\,308\,731$.
10. Nežinoma, ar yra be galo daug x^2+1 pavidalo pirminių skaičių (Landau hipotezė).
11. Nežinoma, ar yra be galo daug pirminių skaičių, lygių trijų sveikųjų skaičių kubų sumai.
12. Nežinoma, ar yra be galo daug aritmetinių progresijų, kurių trys pirmieji nariai – pirminiai skaičiai, kai pirmasis narys – žinomas pirminis skaičius p.

Nežinoma, ar yra be galo daug aritmetinių progresijų su vardikliu 6, kurių trys pirmieji nariai – pirminiai skaičiai (pvz., 5, 11, 17).

13. Nežinoma, ar yra tokių sudėtinių skaičių n, kad su visais a

$$n \mid a^n - a.$$

14. Nežinoma, ar yra be galo daug natūrinių skaičių n, su kuriais

$$p_1 p_2 \ldots p_n + 1$$

yra pirminis skaičius.

15. Nežinoma, ar yra be galo daug tokių natūrinių skaičių n, su kuriais skirtumas

$$2^n - 7$$

yra pirminis skaičius (pvz., kai $n=39$, gauname pirminį skaičių).

16. Surašius pirmuosius n^2 natūrinių skaičių į kvadratinę lentelę iš n eilučių ir n stulpelių, neaišku, ar k-asis stulpelis, kai $(k, n)=1$, ir kiekviena eilutė turės bent vieną pirminį skaičių. Patikrinta, kad teiginys stulpeliams (k-asis stulpelis turi pirminį skaičių, jei $(k, n)=1$) yra teisingas su visais $n \leqslant 100$, o eilutėms – su visais $n \leqslant 4500$.

17. Neaišku, ar yra be galo daug pirminių skaičių, lygių dviejų natūrinių skaičių kubų skirtumui.

18. Nežinoma, ar yra be galo daug pirminių skaičių, lygių trijų natūrinių skaičių kubų sumai.

19. Nežinomas nė vienas pirminis Ferma skaičių F_7 ir F_8 (atitinkamai turinčių 39 ir 78 skaitmenis) daliklis.

20. Nežinoma, ar yra be galo daug pirminių skaičių sekoje

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ \ldots,$$

taip pat neaišku, ar yra toje sekoje be galo daug sudėtinių skaičių.

21. Neaišku, ar, be skaičių 2, 5, 257 (atitinkančių reikšmes $n=1, 2, 4$), yra daugiau n^n+1 pavidalo pirminių skaičių.

22. Nežinoma, ar, be skaičių 3 ir 141, yra daugiau $n \cdot 2^n+1$ pavidalo pirminių skaičių (*Kaleno* skaičių).

23. Neaišku, ar yra be galo daug 2^m+2^n+1 pavidalo ($m>n$ – natūriniai skaičiai) pirminių skaičių (pvz., $2^2+2+1=7$, $2^4+2^2+1=19$).

24. Nežinoma, ar tarp skaičių

$$2+3,\ 2^2+3,\ 2^{2^2}+3,\ 2^{2^{2^2}}+3,\ \ldots$$

yra be galo daug pirminių skaičių.

25. Nežinoma, ar yra be galo daug 2^n+n^2 pavidalo pirminių skaičių (pvz., $17=2^3+3^2$).

26. Neaišku, ar egzistuoja toks natūrinis $a>1$, kad tarp skaičių $a^{2^n}+1$ būtų be galo daug pirminių skaičių.

27. Nežinoma, ar Merseno skaičius M_{M_n} visada pirminis, jei M_n – pirminis Merseno skaičius.

28. Nežinoma, ar visi sekos

$$q_0,\ q_1,\ q_2,\ \ldots,$$

$q_0=2$, $q_{n+1}=2^{q_n}-1$, skaičiai yra pirminiai. Patikrinta, kad yra pirminiai, kai $n \leqslant 4$.

29. Neaišku, ar yra be galo daug pirminių skaičių *Fibonačio* sekoje u_n:

$$u_1=u_2=1,\ u_{n+2}=u_{n+1}+u_n\ (n \geqslant 1).$$

30. Nežinoma, ar yra be galo daug pirminių skaičių sekoje v_n:

$$v_1=1,\ v_2=3,\ v_{n+2}=v_{n+1}+v_n\ \ (n \geqslant 1).$$

Didžiausias žinomas pirminis skaičius $v_{71}=688\ 846\ 502\ 588\ 399$.

31. Neaišku, ar lygtis $2x+1=y$ turi be galo daug pirminių sprendinių (pvz., $x=2$, $y=5$).

32. Nežinoma, ar yra be galo daug stačiųjų trikampių, kurių visų kraštinių ilgiai būtų natūriniai skaičiai, iš kurių du pirminiai (pvz., 3, 4, 5).

33. Nežinoma, ar teisinga *Ferma* hipotezė: jeigu p – pirminis skaičius, tai lygtis

$$x^p+y^p=z^p$$

neišsprendžiama natūriniais skaičiais.

34. Neaišku, ar yra be galo daug iš eilės einančių natūrinių skaičių trejetų, kurių kiekvienas būtų dviejų skirtingų pirminių skaičių sandauga (pvz., 33, 34, 35).

35. Nežinoma, ar iš kiekvieno natūrinio skaičiaus $n\geqslant 10$, pakeitus du jo skaitmenis, galima gauti pirminį skaičių.

36. Neįrodyta *Šincelio* hipotezė: jeigu $x\geqslant 117$, tai tarp x ir $x+\sqrt{x}$ yra bent vienas pirminis skaičius. Hipotezė patikrinta, kai

$$117<x<20\,000\,000.$$

37. Nežinoma, ar yra be galo daug tokių pirminių skaičių p, kad $\frac{p-1}{2}$ taip pat būtų pirminis.

38. Neaišku, ar, imant kiekvieną natūrinį skaičių n, tarp n ir n^3 yra pirminis skaičius.

39. Neįrodyta *Hardy* ir *Litlvudo* hipotezė, kad yra be galo daug pirminių skaičių trejetų: p, $p+2$, $p+6$ (pvz., 11, 13, 17).

40. Nelyginių skaičių sekoje 1, 3, 5, 7, 9, 11, ... pažymėjus $u_1=1$, mažiausias iš skaičių, didesnių už u_1, yra $u_2=3$. Išbraukus kas trečią sekos narį, liks seka

$$1,\ 3,\ 7,\ 9,\ 13,\ \ldots$$

Mažiausias naujos sekos narys, didesnis už u_2, yra $u_3=7$. Išbraukus kas septintą naujos sekos narį, vėl gaunama seka ir t. t. Gautieji skaičiai

$$1,\ 3,\ 7,\ 9,\ 13,\ 15,\ 21,\ 25,\ 31,\ 33,\ 37,\ 43,\ 49,\ 51,\ \ldots$$

vadinami *laimingaisiais*. Nežinoma, ar tarp jų yra be galo daug pirminių skaičių.

Grandininės trupmenos

§18. Racionaliųjų skaičių skleidimas grandininėmis trupmenomis

Kiekvieną racionalųjį skaičių galime išreikšti sveikojo skaičiaus ir teigiamos taisyklingosios trupmenos suma. Pavyzdžiui,

$$-\frac{33}{19} = -2 + \frac{5}{19}.$$

Trupmeną 5/19 išreikškime tokia trupmena, kurios skaitiklis būtų 1:

$$-\frac{33}{19} = -2 + \frac{1}{\frac{19}{5}}.$$

Netaisyklingąją trupmeną vėl galime pakeisti sveikojo skaičiaus ir taisyklingosios trupmenos suma:

$$-\frac{33}{19} = -2 + \frac{1}{3 + \frac{4}{5}}.$$

Tęsdami šį procesą toliau, gauname

$$-\frac{33}{19} = -2 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{4}}}.$$

Tą patį rezultatą galime gauti ir kiek paprasčiau – pasinaudoję Euklido algoritmu. Pritaikykime Euklido algoritmo lygybes skaičiams -33 ir 19:

$$-33 = 19 \cdot (-2) + 5,$$

$$19 = 5 \cdot 3 + 4,$$

$$5 = 4 \cdot 1 + 1,$$

$$4 = 1 \cdot 4.$$

Padalykime kiekvieną lygybę iš atitinkamų vardiklių ir pertvarkykime:

$$-\frac{33}{19}=-2+\frac{5}{19}=-2+\frac{1}{\frac{19}{5}},$$

$$\frac{19}{5}=3+\frac{4}{5}=3+\frac{1}{\frac{5}{4}},$$

$$\frac{5}{4}=1+\frac{1}{4}.$$

Vietoje vardikliuose esančių trupmenų nuosekliai įrašę jų išraiškas iš tolesnių lygybių, gauname „laiptuotą“ trupmeną, kuri lygi sveikojo skaičiaus ir trupmenos sumai. Tos trupmenos skaitiklis lygus 1, o vardiklis vėl lygus sveikojo skaičiaus ir trupmenos sumai ir t. t.

Grandininę trupmeną vadiname reiškinį

$$q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\dots}}}; \qquad (2.1)$$

čia q_i $(i\geqslant 0)$ *– sveikieji skaičiai; visi jie yra teigiami, išskyrus galbūt pirmąjį –* q_0.

Skaičiai q_0, q_1, q_2, ... vadinami grandininės trupmenos *elementais.*

Jeigu (2.1) pavidalo reiškinys lygus skaičiui α (akivaizdu, jog toks α egzistuoja, kai elementų q_i yra baigtinis skaičius), sakome, kad skaičius α *išskleistas grandinine trupmena.*

Jeigu skaičius α išskleistas grandinine trupmena, kurios elementai yra q_0, q_1, q_2, ..., q_n, ..., tai sutrumpintai rašysime

$$\alpha=[q_0,\ q_1,\ q_2,\ \dots,\ q_n,\ \dots].$$

Tas žymėjimas panašus į kelių skaičių mažiausio bendrojo kartotinio žymėjimą, bet kiekvienu atveju iš teksto bus aišku, ką taip žymime.

Grandininė trupmena, turinti begalinį skaičių elementų, vadinama *begaline grandinine trupmena.* Jeigu elementų skaičius baigtinis, tai turime baigtinę grandininę trupmeną. Šio paragrafo pradžioje, skleisdami skaičių $-33/19$, gavome baigtinę grandininę trupmeną, kurią galime užrašyti šitaip:

$$-\frac{33}{19}=[-2,\ 3,\ 1,\ 4].$$

Taikydami Euklido algoritmą, bet kurį racionalųjį skaičių galime išskleisti grandinine trupmena.

30 teorema. *Kiekvienas racionalusis skaičius a/b išskleidžiamas baigtine grandinine trupmena, kurios elementai yra nepilnieji santykiai, gauti Euklido algoritmą taikant skaičiams a ir b.*

Įrodymas. Taikydami Euklido algoritmą skaičiams a ir $b>0$, gauname:

$$\begin{aligned}
a &= q_0 b + r_0, && 0 < r_0 < b,\\
b &= q_1 r_0 + r_1, && 0 < r_1 < r_0,\\
r_0 &= q_2 r_1 + r_2, && 0 < r_2 < r_1,\\
&\cdots\cdots\cdots && \cdots\cdots\cdots\\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}, && 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= q_k r_{k-1}.
\end{aligned}$$

Visas lygybes dalijame iš atitinkamų daliklių ir pertvarkome:

$$\frac{a}{b} = q_0 + \frac{r_0}{b} = q_0 + \frac{1}{\frac{b}{r_0}},$$

$$\frac{b}{r_0} = q_1 + \frac{r_1}{r_0} = q_1 + \frac{1}{\frac{r_0}{r_1}},$$

$$\frac{r_0}{r_1} = q_2 + \frac{r_2}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\frac{r_{k-3}}{r_{k-2}} = q_{k-1} + \frac{r_{k-1}}{r_{k-2}} = q_{k-1} + \frac{1}{\frac{r_{k-2}}{r_{k-1}}},$$

$$\frac{r_{k-2}}{r_{k-1}} = q_k.$$

Vietoje vardikliuose esančių trupmenų nuosekliai įrašome jų reikšmes iš tolesnių lygybių:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cdots\cdots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}};$$

čia visi $q_i>0$ $(i\geqslant 1)$, nes $b>0$ ir $r_i>0$ $(i\geqslant 0)$.

Gauname baigtinę grandininę trupmeną, nes Euklido algoritmas bet kurių dviejų skaičių a ir b porai užbaigiamas ne daugiau kaip po $|b|$ žingsnių (tai jau buvo minėta §4).

Paskutinis grandininės trupmenos elementas $q_k\neq 1$, nes iš $q_k=1$ išplauktų $r_{k-2}=r_{k-1}$, o tai prieštarautų algoritmo sąlygai

$$r_{k-1} < r_{k-2}.$$

Formaliai užrašę grandininę trupmeną, kurios paskutinis elementas 1, galime ją sutrumpinti vienetu padidindami priešpaskutinį elementą, t. y.

$$[q_0, q_1, \ldots, q_{k-2}, q_{k-1}, 1] = [q_0, q_1, \ldots, q_{k-2}, q_{k-1}+1].$$

Tai išplaukia iš grandininės trupmenos apibrėžimo, nes

$$\cfrac{\ldots}{q_{k-2}+\cfrac{1}{q_{k-1}+\cfrac{1}{1}}} = \cfrac{\ldots}{q_{k-2}+\cfrac{1}{q_{k-1}+1}}.$$

Pagal apibrėžimą grandininė trupmena, turinti tik 1 elementą q_0, sutampa su tuo elementu, t. y.

$$[q_0] = q_0.$$

Pravartu įsidėmėti ir šių grandininių trupmenų išraiškas:

$$[q_0, q_1] = q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1}, \tag{2.2}$$

$$[q_0, q_1, q_2] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}} = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1}.$$

§19. Grandininių trupmenų reduktai

Grandininės trupmenos

$$[q_0, q_1, q_2, \ldots, q_{k-1}, q_k, q_{k+1}, \ldots]$$

k-osios eilės reduktu R_k (*k*-uoju reduktu) *vadinama grandininė trupmena*

$$R_k = [q_0, q_1, q_2, \ldots, q_{k-1}, q_k].$$

Taigi reduktus gauname nutraukę grandininę trupmeną ties kažkuriuo elementu.

Pagal redukto apibrėžimą

$$R_0 = [q_0] = q_0,$$

$$R_1 = [q_0, q_1] = \frac{q_0 q_1 + 1}{q_1},$$

$$R_2 = [q_0, q_1, q_2] = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1}$$

ir t. t. Atkreipsime dėmesį, kad k-asis reduktas turi $k+1$ elementą.

Redukto R_k skaitiklį ir vardiklį atitinkamai žymėsime P_k ir Q_k:

$$R_k = \frac{P_k}{Q_k}.$$

Reduktus, kurių indeksai skiriasi 1 ar 2, vadinsime *gretimaisiais*. Gretimųjų reduktų skaitikliai ir vardikliai įvairiai ir įdomiai susiję.

31 teorema. *Grandininės trupmenos*

$$[q_0, q_1, q_2, \ldots, q_k, \ldots]$$

reduktų skaitikliams P_k ir vardikliams Q_k teisingos šios rekurentinės formulės:

$$P_0 = q_0, \quad Q_0 = 1,$$

$$P_1 = q_0 q_1 + 1, \quad Q_1 = q_1,$$

$$P_k = q_k P_{k-1} + P_{k-2},$$

$$Q_k = q_k Q_{k-1} + Q_{k-2} \quad (k \in \mathbf{N},\ k \geqslant 2). \tag{2.3}$$

Rekurentinės formulės teisingos ir kai $k = -1$, jei susitarsime, kad

$$P_{-1} = 1, \quad Q_{-1} = 0. \tag{2.4}$$

Įrodymas. Taikysime indukcijos metodą. Kai $k=2$,

$$P_2 = q_0 q_1 q_2 + q_0 + q_2 = q_2 (q_0 q_1 + 1) + q_0 = q_2 P_1 + P_0,$$

$$Q_2 = q_1 q_2 + 1 = q_2 Q_1 + Q_0.$$

Tarkime, kad (2.3) formulės teisingos k-osios eilės reduktams (turintiems $k+1$ elementą).

Pažymėję

$$\bar{q}_k = q_k + \frac{1}{q_{k+1}},$$

galime užrašyti:

$$R_{k+1} = [q_0, q_1, \ldots, q_{k-1}, q_k, q_{k+1}] = [q_0, q_1, \ldots, q_{k-1}, \bar{q}_k].$$

Akivaizdu, jeigu k-osios eilės redukte R_k paskutinį elementą q_k pakeisime skaičiumi $\bar{q}_k$, tai gausime reduktą R_{k+1}. Skaičiai P_{k-1}, P_{k-2}, Q_{k-1}, Q_{k-2} išreiškiami elementais $q_0, q_1, \ldots, q_{k-1}$ naudojantis rekurentinėmis formulėmis, jie nepriklauso nuo elemento q_k. Todėl elementą q_k pakeitus skaičiumi $\bar{q}_k$, reduktų R_{k-1} ir R_{k-2} skaitiklių ir vardiklių išraiškos nepasikeičia.

Vadinasi, užrašę reduktą R_{k+1} vienu elementu trumpesnės grandininės trupmenos pavidalu, galime taikyti indukcijos prielaidą. Gauname

$$R_{k+1} = \frac{\bar{q}_k P_{k-1} + P_{k-2}}{\bar{q}_k Q_{k-1} + Q_{k-2}} = \frac{\left(q_k + \frac{1}{q_{k+1}}\right) P_{k-1} + P_{k-2}}{\left(q_k + \frac{1}{q_{k+1}}\right) Q_{k-1} + Q_{k-2}} =$$

$$= \frac{q_{k+1}(q_k P_{k-1} + P_{k-2}) + P_{k-1}}{q_{k+1}(q_k Q_{k-1} + Q_{k-2}) + Q_{k-1}} = \frac{q_{k+1} P_k + P_{k-1}}{q_{k+1} Q_k + Q_{k-1}}.$$

Taigi ir $k+1$-ojo redukto skaitikliams ir vardikliams teisingos (2.3) formulės. Teorema įrodyta.

Naudodamiesi rekurentinėmis (2.3) formulėmis, galime nuosekliai apskaičiuoti visų eilių reduktų skaitiklius ir vardiklius. Patogiausia tai atlikti sudarant atitinkamą lentelę, kurios pirmojoje eilutėje rašome eilės numerį, antrojoje — grandininės trupmenos elementus q_k, trečiojoje ir ketvirtojoje — atitinkamai reduktų skaitiklius P_k ir vardiklius Q_k. Pirmasis skaičių stulpelis, pažymėtas numeriu -1, skirtas (2.4) lygybėmis apibrėžtiems pagalbiniams dydžiams P_{-1} ir Q_{-1}. Antrajame stulpelyje rašome reikšmes, vienodas bet kuriai grandininei trupmenai: $P_0=q_0$, $Q_0=1$. Paskutines dvi eilutes užpildome taikydami iš rekurentinių (2.3) formulių išplaukiančias taisykles: jeigu radome skaitiklius P_{k-2}, P_{k-1}, tai P_k randame padauginę elementą q_k iš skaitiklio P_{k-1} ir prie sandaugos pridėję P_{k-2}, o Q_k randame padauginę q_k iš Q_{k-1} ir prie sandaugos pridėję Q_{k-2}.

Jeigu skaičius α išskleistas baigtine grandinine trupmena:

$$\alpha=[q_0, q_1, q_2, \ldots, q_k],$$

tai jis sutampa su savo paskutiniu reduktu R_k. Taigi naudodamiesi tokia lentele, galime rasti ir skaičiaus, užrašyto baigtine grandinine trupmena, išraišką paprastąja trupmena.

Pavyzdys. Rasime skaičiaus, užrašyto baigtine grandinine trupmena $\alpha=[2, 1, 1, 2, 3, 2]$, išraišką paprastąja trupmena.

k	-1	0	1	2	3	4	5
q_k		2	1	1	2	3	2
P_k	1	2	3	5	13	44	101
Q_k	0	1	1	2	5	17	39

Radome $P_2=5$, $P_1=3$. P_2 dauginame iš elemento $q_3=2$, prie gautos sandaugos pridedame $p_1=3$ ir gauname $p_3=13$. Naudodamiesi lentele, randame visus reduktus:

$$R_0=2,\quad R_1=3,\quad R_2=\frac{5}{2},\quad R_3=\frac{13}{5},\quad R_4=\frac{44}{17},\quad R_5=\frac{101}{39}.$$

Palyginę (2.3) rekurentines formules su 4 paragrafe pateiktomis (1.8) formulėmis, kuriomis apibrėžti Oilerio skliaustai, matome, kad reduktų skaitikliai ir vardikliai išreiškiami atitinkamais Oilerio skliaustais. Būtent, teisingos šitokios lygybės:

$$P_k=((q_0, q_1, q_2, \ldots, q_k)),$$
$$Q_k=((q_1, q_2, \ldots, q_k)), \qquad (2.3a)$$

kai $k\geqslant 1$.

Lentelės, kuriomis naudojantis I skyriaus pavyzdžiuose buvo skaičiuojamos Oilerio skliaustų reikšmės, buvo užpildomos pagal tą pačią taisyklę, kaip ir ką tik pateikta lentelė. Pastaroji skiriasi tik vienu papildomu stulpeliu, atitinkančiu reikšmę $k=-1$.

32 teorema. *Grandininės trupmenos gretimųjų reduktų skaitikliai ir vardikliai susieti lygybe*

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}. \tag{2.5}$$

Įrodymas. Įrodysime indukcijos metodu. Kai $k=1$,

$$P_1 Q_0 - P_0 Q_1 = (q_0 q_1 + 1) \cdot 1 - q_0 \cdot q_1 = 1.$$

Taigi šiuo atveju (2.5) formulė yra teisinga. Tarkime, kad ji teisinga su bet kuriuo k. Tuomet, pakeitę k skaičiumi $k+1$, turime

$$P_{k+1} Q_k - P_k Q_{k+1} = (q_{k+1} P_k + P_{k-1}) Q_k - P_k (q_{k+1} Q_k + Q_{k-1}) =$$
$$= P_{k-1} Q_k - P_k Q_{k-1} = (-1)^k = (-1)^{(k+1)-1}.$$

Skaičiams P_{k+1} ir Q_{k+1} taikėme (2.3) rekurentines formules. Teorema įrodyta.

Išvada. *Bet kuris reduktas yra nesuprastinama trupmena.*
Iš tikrųjų, jeigu $(P_k, Q_k) = d$, tai iš (2.5) gauname

$$d \mid (-1)^{k-1} \Rightarrow d = 1.$$

Taigi norėdami suprastinti trupmeną, turime ją išskleisti grandinine trupmena ir rasti jos paskutinį reduktą, lygų suprastintai trupmenai.

Uždaviniai

1. Išskleiskite grandinine trupmena šiuos skaičius:

$$\frac{125}{31},\ \frac{49}{45},\ \frac{95}{201},\ 1{,}12,\ \frac{1}{1{,}21},\ \frac{411}{144},\ \frac{1882}{1651}.$$

2. Suprastinkite skleisdami grandininėmis trupmenomis:

$$\frac{326}{318},\ \frac{174}{222},\ \frac{3587}{2743},\ \frac{2086}{6854}.$$

3. Raskite grandininių trupmenų reikšmes:

$[1, 2, 3, 4, 5]$, $[1, 1, 2, 1, 1, 2, 2]$, $[1, 1, 1, 1, 1, 2, 2, 2, 2, 3]$.

4. Raskite šių grandininių trupmenų reikšmes:

$[a, b, c, d]$, $[a, a, a, a, b]$, $[a, b, a, b, a, b]$, $[a, b, b, b, b, a]$,

5. Išspręskite šias lygtis:

$$[x, 1, 1, 2] = \frac{18}{5},\quad [1, 1, 2, x] = \frac{27}{16},\quad [2, 1, x, 1, 2] = \frac{21}{8},$$

$$3(xyz + x + z) = 5(yz + 1).$$

6. Išskleiskite grandinine trupmena šiuos skaičius:

$$-3{,}1,\quad (-3/7)^{-2},\quad 0{,}025,\quad 1 + \frac{2}{135},\quad 5 - \frac{1}{25}.$$

7. Užrašykite visus grandininės trupmenos

$$[1, 1, 1, 1, 2, 1, 1, 1, 2]$$

reduktus ir išdėstykite juos didėjimo tvarka.

§20. Reduktų savybės

33 teorema. *Grandininės trupmenos reduktus sieja šitokie sąryšiai:*

$$P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k q_k \quad (k \geqslant 2), \tag{2.6}$$

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^{k-1}}{Q_k Q_{k-1}} \quad (k \geqslant 1), \tag{2.7}$$

$$\frac{P_k}{Q_k} - \frac{P_{k-2}}{Q_{k-2}} = \frac{(-1)^k q_k}{Q_k Q_{k-2}} \quad (k \geqslant 2). \tag{2.8}$$

Įrodymas. (2.6) lygybė įrodoma gana paprastai:

$$P_k Q_{k-2} - P_{k-2} Q_k = (q_k P_{k-1} + P_{k-2}) Q_{k-2} - P_{k-2} (q_k Q_{k-1} + Q_{k-2}) =$$
$$= q_k (P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1}) = (-1)^{k-2} q_k = (-1)^k q_k.$$

Kitos dvi lygybės išplaukia iš (2.5) ir (2.6) lygybių.

34 teorema. *Reduktų vardikliai sudaro monotoniškai didėjančių teigiamųjų skaičių seką.*

Įrodymas. Taikysime indukcijos metodą. Jeigu $k=2$, tai

$$Q_2 = q_2 Q_1 + Q_0 = q_2 q_1 + 1 > q_1 = Q_1 > 0.$$

Tarkime, kad teoremos tvirtinimas teisingas reduktams iki k-osios eilės. Tuomet $k+1$-ojo redukto vardiklis

$$Q_{k+1} = q_{k+1} Q_k + Q_{k-1} > Q_k > 0.$$

Teorema įrodyta.

Gali sutapti tik Q_1 ir Q_0, kai $Q_1 = 1$. Kitais atvejais vardikliai nelygūs — didesnio indekso redukto vardiklis didesnis už mažesnio indekso redukto vardiklį.

1 išvada. *Lyginės eilės reduktai sudaro didėjančią seką.*

Įrodymas išplaukia iš (2.8) formulės. Jeigu k — lyginis skaičius, tai dešiniojoje lygybės pusėje — teigiamasis skaičius. Taigi

$$\frac{P_{2k}}{Q_{2k}} > \frac{P_{2k-2}}{Q_{2k-2}}. \tag{2.9}$$

2 išvada. *Nelyginės eilės reduktai sudaro mažėjančią seką*

$$\frac{P_{2k+1}}{Q_{2k+1}} < \frac{P_{2k-1}}{Q_{2k-1}}. \tag{2.10}$$

Tuo įsitikiname (2.8) lygybėje indeksą k pakeitę nelyginiu skaičiumi $2k+1$.

3 išvada. *Iš dviejų gretimųjų reduktų lyginės eilės reduktas mažesnis už nelyginės eilės reduktą*:

$$\frac{P_{2k}}{Q_{2k}} < \frac{P_{2k-1}}{Q_{2k-1}}, \tag{2.11}$$

$$\frac{P_{2k}}{Q_{2k}} < \frac{P_{2k+1}}{Q_{2k+1}}. \tag{2.12}$$

Abi tas nelygybes galime gauti iš (2.7) lygybės, vieną kartą k pakeitę lyginiu skaičiumi $2k$, kitą kartą – nelyginiu skaičiumi $2k+1$.

Visais tais atvejais, nustatydami (2.7)–(2.8) lygybių dešiniųjų pusių ženklus, rėmėmės 34 teoremos teiginiu, kad reduktų vardikliai yra teigiamieji skaičiai.

4 išvada. *Bet kuris lyginės eilės* $2s$ *reduktas mažesnis už bet kurį nelyginės eilės* $2r+1$ *reduktą.*

Teiginio teisingumas išplaukia iš jau įrodytų 1–3 išvadų bei šių nelygybių:

$$R_{2s} \leqslant R_{2s+2r} < R_{2s+2r+1} \leqslant R_{2r+1}.$$

Skaičiaus skleidinio α grandinine trupmena

$$\alpha = [q_0, q_1, q_2, \ldots, q_{k-1}, q_k, q_{k+1}, \ldots]$$

k-osios eilės liekana r_k vadinsime grandininę trupmeną

$$r_k = [q_k, q_{k+1}, \ldots].$$

Pagal apibrėžimą

$$\alpha = r_0,$$

$$\alpha = [q_0, r_1],$$

$$\alpha = [q_0, q_1, r_2],$$

$$\alpha = [q_0, q_1, q_2, \ldots, q_{k-1}, r_k].$$

Jeigu skaičiaus α grandininė trupmena turi k elementų (paskutinis iš jų yra q_{k-1}), tai $r_s = 0$ $(s \geqslant k)$.

35 teorema. *Grandininė trupmena* α, *kurios* k*-oji liekana* $r_k \neq 0$, *išreiškiama šitaip*:

$$\alpha = \frac{P_{k-1} r_k + P_{k-2}}{Q_{k-1} r_k + Q_{k-2}}. \tag{2.13}$$

Įrodymas. Užrašytoji formulė teisinga, kai r_k – sveikasis skaičius. Tai išplaukia iš (2.3) rekurentinių formulių. Šį atvejį atitinkančią grandininės trupmenos reikšmę žymėsime α^*. Iš tų pačių rekurentinių formulių išplaukia, kad skaičiai P_{k-1}, P_{k-2}, Q_{k-1}, Q_{k-2} nepriklauso nuo grandininės trupmenos elementų, kurių indeksai didesni už $k-1$, taigi jie nepriklauso ir nuo r_k. Pakeitę sveikąją r_k reikšmę dydžiu $[q_k, q_{k+1}, \ldots]$, iš α^* gauname skaičių α, o skaičiai P_{k-1}, P_{k-2}, Q_{k-1}, Q_{k-2} nepasikeičia. Todėl (2.13) formulė teisinga bet kokiai r_k reikšmei.

36 teorema. *Visi skaičiaus α grandininės trupmenos lyginės eilės reduktai mažesni už α, o nelyginės eilės reduktai didesni už α, išskyrus paskutinį reduktą, kuris sutampa su α.*

Taigi teisingos nelygybės

$$R_0 < R_2 < \ldots < R_{2k} < \ldots < \alpha < \ldots < R_{2k-1} < \ldots < R_3 < R_1. \quad (2.14)$$

Įrodymas. Naudodamiesi (2.13) formule, skaičių α išreiškiame liekana $r_{k+1} \neq 0$. Tada

$$\alpha - R_{k-1} = \frac{P_k r_{k+1} + P_{k-1}}{Q_k r_{k+1} + Q_{k-1}} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^{k-1} r_{k+1}}{(Q_k r_{k+1} + Q_{k-1}) Q_{k-1}}, \quad (2.15)$$

$$\alpha - R_k = \frac{P_k r_{k+1} + P_{k-1}}{Q_k r_{k+1} + Q_{k-1}} - \frac{P_k}{Q_k} = \frac{(-1)^k}{(Q_k r_{k+1} + Q_{k-1}) Q_k}. \quad (2.16)$$

Jeigu k – lyginis skaičius, tai iš (2.16) išplaukia

$$\alpha > R_{2k},$$

jeigu k – nelyginis, tai priešingo ženklo nelygybė.

Išvada.

$$|\alpha - R_k| < |\alpha - R_{k-1}|. \quad (2.17)$$

Įrodymas. Pakanka palyginti (2.15) ir (2.16) lygybių dešiniąsias puses ir prisiminti, kad $Q_k > Q_{k-1}$, $r_{k+1} \geqslant q_{k+1} \geqslant 1$.

Pagal 36 teoremą reduktai, didėjant jų indeksui, artėja prie skaičiaus α: nelyginiai iš dešinės, lyginiai iš kairės. Kuo didesnis indeksas, tuo mažesnis skirtumas tarp redukto R_k ir skaičiaus α.

Iki šiol nagrinėjome tik baigtines grandinines trupmenas, kuriomis, remdamiesi 30 teorema, reiškėme racionaliuosius skaičius. Kadangi kiekviena baigtinė grandininė trupmena lygi racionaliajam skaičiui (paskutiniam reduktui), tai iracionalieji skaičiai negali būti išreikšti baigtinėmis grandininėmis trupmenomis. Kitame paragrafe matysime, kad tie skaičiai išreiškiami begalinėmis grandininėmis trupmenomis.

Nagrinėsime, ar turi prasmę begalinė grandininė trupmena.

37 teorema. *Begalinės grandininės trupmenos reduktų seka turi ribą.*

Įrodymas. Sudarysime seką uždarųjų intervalų, kurių kairieji galai yra lyginės eilės reduktai, o dešinieji – vienetu didesnio indekso nelyginės eilės reduktai:

$$[R_0, R_1], \quad [R_2, R_3], \quad [R_4, R_5], \quad \ldots \quad (2.18)$$

Iš 34 teoremos išvadų išplaukia, kad tie intervalai sudaro susitraukiančiųjų intervalų seką. Būtent, bet kuris intervalas, pradedant antruoju, yra prieš jį einančio intervalo dalis. Be to, remiantis 34 teorema,

$$\lim_{n \to \infty} Q_n = \infty$$

ir

$$\lim_{n\to\infty} |R_{n+1}-R_n| = \lim_{n\to\infty} \frac{1}{Q_{n+1}Q_n} = 0.$$

Matome, kad (2.18) sekos intervalų ilgiai, kai n didėja, nuosekliai mažėja ir artėja prie nulio. Lieka remtis matematinės analizės teorema, tvirtinančia, kad susitraukiančiųjų intervalų seka turi bendrą tašką. Tas taškas šiuo atveju yra lyginės ir nelyginės eilės reduktų sekų bendras ribinis taškas.

Uždaviniai

8. Užrašykite formulę skirtumui R_k-R_{k-4} skaičiuoti.

9. Raskite visas grandininių trupmenų [1, 2, 3, 4], [1, 1, 5, 1, 1, 2], [1, 1, 1, 1, 1, 1, 1, 7] ir visų jų liekanų reikšmes.

10. Įvertinkite skirtumus tarp skaičių ir jų visų eilių reduktų, kai: a) $\alpha=[-2, 1, 1, 1, 4]$; b) $\beta=[1, 3, 4, 2]$; c) $\gamma=[0, 5, 3, 2]$.

11. Užrašykite visas trupmenas, kurių vardikliai ne didesni už 10 ir kurios nutolusios nuo skaičaus $\alpha=[2, 1, 1, 3]$ ne daugiau kaip vieneto atstumu. Ar yra tarp jų skaičiaus α reduktų?

12. Skaičiaus α paskutinis reduktas yra $R_3=23/9$, o $R_1=3$. Raskite skaičių R_2.

13. Užrašykite visus galimus racionaliuosius skaičius, kurių reduktų vardikliai Q_k $(k>0)$ būtų tik vienaženkliai pirminiai skaičiai.

§21. Realiųjų skaičių skleidimas grandininėmis trupmenomis

Ieškodami racionaliojo skaičiaus skleidinio grandinine trupmena, Euklido algoritmo negalime taikyti. Todėl aptarsime kitą būdą, kuris išplaukia iš šios teoremos.

38 teorema. *Kiekvieną realųjį skaičių α galima išskleisti grandinine trupmena vieninteliu būdu.*

Įrodymas. Skaičiaus α skleidinio grandinine trupmena pirmuoju elementu imame skaičiaus α sveikąją dalį $q_0=[\alpha]$. Jeigu skaičiaus α trupmeninė dalis $\{\alpha\}$ lygi 0, tai skaičiaus α skleidimas grandinine trupmena baigtas. Jeigu $\{\alpha\}>0$, tai α_1 žymime dydį, atvirkštinį skaičiaus α trupmeninei daliai. Tada

$$\alpha = q_0 + \frac{1}{\alpha_1}.$$

Iš $0<\{\alpha\}<1$ išplaukia, kad

$$1 < \alpha_1 = \frac{1}{\{\alpha\}}. \tag{2.19}$$

Vadinasi, skaičiaus α_1 sveikoji dalis q_1 yra natūrinis skaičius. Jeigu $\{\alpha_1\}=0$, tai skaičius α yra išskleistas grandinine trupmena:

$$\alpha = [q_0, q_1].$$

Priešingu atveju, kai $\{\alpha\}>0$, α_2 žymime dydį, atvirkštinį skaičiaus α_1 trupmeninei daliai. Tada

$$\alpha_1 = q_1 + \frac{1}{\alpha_2}.$$

α_2 didesnis už 1 kaip dydis, atvirkštinis skaičiaus α_1 trupmeninei daliai. Tęsdami tą procesą, gausime

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \dots}} = [q_0,\ q_1,\ q_2,\ \dots].$$

Šioje grandininėje trupmenoje visi $q_i \geqslant 1$ $(i > 0)$ – tai išplaukia iš (2.19) tipo nelygybių. Skleidinio vienatis išplaukia iš to, kad bet kurio skaičiaus sveikoji ir trupmeninė dalys randamos vienareikšmiškai.

Kai α – iracionalusis skaičius, skleidimo procesas negali pasibaigti, nes priešingu atveju gautume prieštaravimą: iracionalusis skaičius būtų lygus racionaliajam skaičiui (savo paskutiniam reduktui). Taigi tik iracionalieji skaičiai išskleidžiami begalinėmis grandininėmis trupmenomis.

Pavyzdys. Išskleisime grandinine trupmena lygties $x^3 - 2 = 0$ šaknį. Kadangi kairioji lygties pusė neigiama, kai $x = 1$, ir teigiama, kai $x = 2$, tai šaknis yra tarp 1 ir 2, jos sveikoji dalis lygi 1. Pažymėję

$$x = 1 + \frac{1}{y}$$

ir įrašę į lygtį vietoj x, gauname kubinę lygtį

$$\left(1 + \frac{1}{y}\right)^3 - 2 = 0.$$

Ją padauginę iš y^3, gauname

$$f_1(y) = y^3 - 3y^2 - 3y - 1 = 0.$$

Kadangi $f_1(3) = -10 < 0$, o $f_1(4) = 3 > 0$, tai $[y] = 3$ ir

$$y = 3 + \frac{1}{z}.$$

Vietoj y įrašę $3 + 1/z$, gauname lygtį

$$f_2(z) = 10z^3 - 6z^2 - 6z - 1 = 0.$$

Panašiai randame $[z] = 1$ ir t. t.

Taigi gavome tris $\sqrt[3]{2}$ skleidinio grandinine trupmena elementus: $q_0 = 1$, $q_1 = 3$, $q_2 = 1$. Todėl

$$\sqrt[3]{2} = [1,\ 3,\ 1,\ \dots].$$

Panašiai rastume ir kitus elementus q_i. Tačiau, kaip taisyklė, atitinkamų lygčių koeficientai didėja, skaičiavimai darosi sudėtingi ir anksčiau ar vėliau viršija skaičiuotojų (ar kompiuterių) galimybes. Antra vertus, remiantis rastaisiais elementais q_i nepavyksta iškelti vienokios ar kitokios hipotezės apie $\sqrt[3]{2}$ grandininės trupmenos elementų dėsningumus. Beje, šios pastabos tinka ne tik skaičiui $\sqrt[3]{2}$. Labai siaura yra klasė skaičių, kurių skleidimas grandinine trupmena nekelia problemų. Tai – racionalieji skaičiai, kvadratinės iracionalybės. Kitokio tipo skaičių nemokame išskleisti grandinine trupmena, nors yra viena kita išimtis.

1737 m. L. Oileriui pasisekė išskleisti grandinine trupmena skaičių

$$\frac{e^{x/k}+1}{e^{x/k}-1}.$$

Oileriui priklauso ir skleidimo dėsnio

$$\frac{e+1}{e-1}=[2,\ 6,\ 10,\ \ldots,\ 4n+2,\ \ldots]$$

įrodymas (jis buvo pateiktas vadovėlio 1-ajame leidime).

L. Oileris taip pat rado skaičiaus e grandininę trupmeną:

$$e=[2,\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6,\ 1,\ 1,\ 8,\ \ldots],$$

t. y.

$$q_0=2,\quad q_{3n}=q_{3n+1}=1,\quad q_{3n-1}=2n\ \ (n\geqslant 1).$$

G. Lochsas apskaičiavo 969 skaičiaus π grandininės trupmenos elementus, didžiausias iš jų yra 20 776. Skaičius 1 pasikartoja 393 kartus. Skaičiaus π skleidinio pirmieji elementai yra šie:

$$\pi=[3,\ 7,\ 15,\ 1,\ 292,\ 1,\ 1,\ 1,\ 2,\ 1,\ 3,\ 1,\ 14,\ 2,\ 1,\ 1,\ 2,$$
$$2,\ 2,\ 2,\ 1,\ 84,\ 2,\ 1,\ 1,\ 15,\ 3,\ 13,\ 1,\ 4,\ \ldots].$$

1971 m. amerikiečių mokslininkai *S. Lengas* ir *H. Troteris*, naudodamiesi kompiuteriais, apskaičiavo 1000 skaičiaus $\sqrt[3]{2}$ grandininės trupmenos elementų. Pirmieji 50 elementų yra šitokie:

$$\sqrt[3]{2}=[1,\ 3,\ 1,\ 5,\ 1,\ 1,\ 4,\ 1,\ 1,\ 8,\ 1,\ 14,\ 1,\ 10,\ 2,\ 1,\ 4,\ 12,$$
$$2,\ 3,\ 2,\ 1,\ 3,\ 4,\ 1,\ 1,\ 2,\ 14,\ 3,\ 12,\ 1,\ 15,\ 3,\ 1,\ 4,$$
$$534,\ 1,\ 1,\ 5,\ 1,\ 1,\ 121,\ 1,\ 2,\ 2,\ 4,\ 10,\ 3,\ 2,\ 2,\ \ldots].$$

Atlikta ir daugiau panašių skaičiavimų, tačiau jų čia nepateiksime.

Uždaviniai

14. Raskite 4 skaičiaus $\sqrt[3]{3}$ skleidinio grandinine trupmena elementus.

15. Apskaičiuokite pirmuosius 6 skaičiaus e skleidinio reduktus. Kokiu tikslumu R_5 išreiškia šį skaičių?

16. Raskite mažiausią natūrinį skaičių n, su kuriuo R_n yra skaičiaus π artinys 10^{-6} tikslumu.

17. Raskite skaičių $2\sqrt{3}$, $\sqrt{5}-1$, $2-\sqrt{2}$ skleidinių grandininėmis trupmenomis pirmuosius 5 elementus.

18. Raskite po 10 skaičių $\sqrt[3]{3}$ ir $-\sqrt[3]{3}$ skleidinių grandininėmis trupmenomis elementų. Ar galite nurodyti dėsningumą, siejantį abi tas grandinines trupmenas?

§22. Dirichlė teorema

Šiame paragrafe nagrinėsime, kokiu tikslumu reduktais galime pakeisti skaičius, išskleistus grandinine trupmena.

39 teorema. *Skaičiaus α skleidinio grandinine trupmena reduktams teisingos nelygybės*:

$$\left| \alpha - \frac{P_k}{Q_k} \right| \leqslant \frac{1}{Q_k Q_{k+1}}, \tag{2.20}$$

$$\left| \alpha - \frac{P_k}{Q_k} \right| \leqslant \frac{1}{Q_k^2}, \tag{2.21}$$

$$\left| \alpha - \frac{P_k}{Q_k} \right| > \frac{1}{Q_k (Q_k + Q_{k+1})} \quad (\alpha \neq R_k). \tag{2.22}$$

Įrodymas. Reduktai R_k ir R_{k+1} yra su skirtingo lyginumo indeksais ir skirtingose skaičiaus α pusėse (35 teorema). Todėl skirtumas $|\alpha - R_k|$ mažesnis už skirtumą $|R_{k+1} - R_k|$ (lygybė galima, kai $\alpha = R_{k+1}$):

$$\left| \alpha - \frac{P_k}{Q_k} \right| \leqslant \left| \frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} \right| = \frac{1}{Q_k Q_{k+1}}.$$

Prisiminę, kad $Q_{k+1} \geqslant Q_k$, iš (2.20) gauname (2.21).

Norėdami įrodyti paskutinę nelygybę, pastebėsime, kad R_k ir R_{k+2} yra su vienodo lyginumo indeksais, abu yra vienoje skaičiaus α pusėje. Jeigu $\alpha \neq R_{k+2}$, tai

$$\left| \alpha - \frac{P_k}{Q_k} \right| > \left| \frac{P_{k+2}}{Q_{k+2}} - \frac{P_k}{Q_k} \right| = \frac{q_{k+2}}{Q_k Q_{k+2}} = \frac{q_{k+2}}{Q_k (q_{k+2} Q_{k+1} + Q_k)} =$$

$$= \frac{1}{Q_k \left(Q_{k+1} + \dfrac{Q_k}{q_{k+2}} \right)} \geqslant \frac{1}{Q_k (Q_{k+1} + Q_k)},$$

o jeigu $\alpha = R_{k+2}$, tai

$$\left| \alpha - \frac{P_k}{Q_k} \right| = \left| \frac{P_{k+2}}{Q_{k+2}} - \frac{P_k}{Q_k} \right| > \frac{1}{Q_k (Q_{k+1} + Q_k)},$$

nes pastaruoju atveju $q_{k+2} > 1$ (kaip paskutinis grandininės trupmenos elementas).

Vokiečių matematikas P. Dirichlė įrodė šią teoremą.

40 (Dirichlė) teorema. *Imant bet kurį realųjį skaičių α ir bet kurį $\tau > 0$, galima rasti tokią trupmeną a/b, kurios vardiklis $b \leqslant \tau$ ir*

$$\left| \alpha - \frac{a}{b} \right| < \frac{1}{b\tau}. \tag{2.23}$$

Įrodymas. Išskleisime α grandinine trupmena. Jeigu yra toks indeksas k, kad $Q_k \leqslant \tau < Q_{k+1}$, tai trupmeną a/b galime laikyti lygia R_k, nes

$$\left| \alpha - \frac{a}{b} \right| = \left| \alpha - \frac{P_k}{Q_k} \right| \leqslant \frac{1}{Q_k Q_{k+1}} < \frac{1}{Q_k \tau} = \frac{1}{b\tau}.$$

Redukto vardiklio $Q_{k+1} > \tau$ negalime rasti tuomet, kai skaičius α yra racionalus ir sutampa su savo paskutiniu reduktu P_k/Q_k, kurio vardiklis $Q_k < \tau$. Tačiau tada

$$\left| \alpha - \frac{P_k}{Q_k} \right| = 0 < \frac{1}{Q_k \tau} = \frac{1}{b\tau}.$$

Teorema įrodyta.

Iš teoremos teiginio išplaukia, kad bet kurį realųjį skaičių galime pakeisti jo racionaliuoju artiniu a/b, darydami paklaidą, ne didesnę už skaičių, atvirkštinį vardiklio kvadratui. Patogiausia tokia trupmena imti atitinkamą reduktą. Remdamiesi (2.20)–(2.22) nelygybėmis, galime nustatyti daromos paklaidos dydį.

Pavyzdys. Išreikšime natūrinių logaritmų pagrindą e racionaliuoju skaičiumi 0,001 tikslumu. Naudosimės žinomu e skleidiniu grandinine trupmena:

$$e = [2, 1, 2, 1, 1, 4, 1, \ldots].$$

Sudarome lentelę reduktams skaičiuoti:

	2	1	2	1	1	4	1
1	2	3	8	11	19	87	106
0	1	1	3	4	7	32	39

Skaičiaus e skleidinio reduktas $R_5 = 87/32$ ir yra skaičiaus e artinys 0,001 tikslumu, nes

$$|e - R_5| < \frac{1}{Q_5 Q_6} = \frac{1}{32 \cdot 39} = \frac{1}{1248} < 0{,}001.$$

Uždaviniai

19. Raskite skaičius $12 - 12^{-1}$, $-0{,}0125$, $[1, 4, 4, 2]$, π atitinkančias trupmenas, nurodytas Dirichlė teoremoje, kai $\tau = 10^{-3}$.

20. Raskite visas skaičių $\pi + 2$ atitinkančias trupmenas, nurodytas Dirichlė teoremoje, kai $\tau = 10^{-2}$.

21. Raskite skirtumo $|\alpha - R_5|$ didumą, kai $\alpha = [2, 1, 1, 3, 1, 1, 5]$.

22. Įvertinkite skirtumą $|e - R_i|$ iš viršaus ir iš apačios, kai $i = 4, 5, 6$.

23. Naudodamiesi grandininėmis trupmenomis, apskaičiuokite 10^{-4} tikslumu šiuos skaičius:

$$2\sqrt{5}, \quad \sqrt{21}, \quad \sqrt{19}, \quad 3\sqrt{7} - 4, \quad \sqrt[3]{3}.$$

§23. Geriausieji artiniai

Neretai įvairiuose skaičiavimuose iracionaliuosius skaičius tenka keisti jiems artimais racionaliaisiais skaičiais. Stengiamasi parinkti tokį racionalųjį skaičių, kuris kiek galima tiksliau išreikštų iracionalųjį skaičių. Tačiau tikslumas nėra vienintelis kriterijus parenkant skaičiaus artinį. Dažnai patogiau vietoj tikslesnio, bet gremėzdiškos išraiškos artinio imti kitą, gal ne tiek tikslų, bet paprastesnį, patogesnės išraiškos skaičių. Pavyzdžiui, trupmena 3,142 išreiškia skaičių π 10^{-3} tikslumu, o trupmena $22/7$ – tik $1/700$ tikslumu,

tačiau pastaroji yra paprastesnė ir todėl kartais patogesnė. Atsižvelgdami į abu kriterijus, apibrėšime *geriausiojo artinio* sąvoką.

Racionalusis skaičius a/b vadinamas realiojo skaičiaus α geriausiuoju artiniu, jei nėra trupmenos x/y, $1 \leqslant y \leqslant b$, su kuria būtų teisinga nelygybė

$$\left| \alpha - \frac{x}{y} \right| < \left| \alpha - \frac{a}{b} \right|.$$

Kitaip tariant, jeigu visų trupmenų, esančių arčiau skaičiaus α negu trupmena a/b, vardikliai didesni už b, tai trupmena a/b vadinama skaičiaus α geriausiuoju artiniu.

Nagrinėjant geriausius artinius, labai praverčia ši teorema, kuri įdomi ir pati savaime.

41 teorema. *Jeigu uždarojo intervalo galai yra trupmenos a/b, c/d, tenkinančios sąlygą*

$$bc - ad = 1, \tag{2.24}$$

tai:

1) *bet kurios trupmenos x/y, priklausančios tam intervalui, vardiklis didesnis už skaičius d ir b,*

2) *bet kurio realiojo skaičiaus α, priklausančio tam intervalui, geriausiasis artinys yra tam skaičiui artimesnis intervalo galas.*

Įrodymas. Tarkime, kad

$$\frac{a}{b} < \frac{x}{y} < \frac{c}{d}. \tag{2.25}$$

Tuomet

$$\frac{x}{y} - \frac{a}{b} = \frac{bx - ay}{by} \geqslant \frac{1}{by},$$

nes sveikas teigiamasis skaičius $bx - ay \geqslant 1$. Kita vertus,

$$\frac{x}{y} - \frac{a}{b} < \frac{c}{d} - \frac{a}{b} = \frac{1}{bd},$$

nes skirtumas $bc - ad$ pagal teoremos sąlygą lygus 1. Taigi

$$\frac{1}{by} < \frac{1}{bd}$$

ir todėl $y > b$.

Panašiai galima įrodyti nelygybę $y > d$.

Antrasis teoremos tvirtinimas išplaukia iš pirmojo ir iš geriausiųjų artinių apibrėžimo.

Išvada. *Skaičiaus α geriausiasis artinys yra kiekvienas jo skleidinio reduktas.*

Norint įrodyti, kad reduktas R_k yra skaičiaus α artinys, užtenka imti intervalą, kurio galai yra reduktai R_k, R_{k-1}. Pagal 32 teoremą to intervalo galai tenkina (2.24) sąlygą. Reduktas R_k yra arčiau skaičiaus α negu reduktas R_{k-1} (36 teoremos išvada), todėl R_k yra geriausiasis artinys.

42 (geriausiųjų artinių) teorema. *Visi realiojo skaičiaus*

$$\alpha=[q_0, q_1, q_2, \ldots, q_k, \ldots]$$

geriausieji artiniai yra šitokio pavidalo skaičiai:

$$\gamma_x=\frac{P_k x+P_{k-1}}{Q_k x+Q_{k-1}}; \tag{2.26}$$

čia x – sveikasis skaičius, $0\leqslant x\leqslant q_{k+1}$.

Teoremos neįrodinėsime (ji buvo įrodyta vadovėlio 1-ajame leidime).

Teorema netvirtina, kad visi nurodytojo pavidalo skaičiai yra geriausieji artiniai.

Pavyzdys. Rasime skaičiaus π geriausiuosius artinius, kurių vardikliai ne didesni už 60. Žinome, kad

$$\pi=[3, 7, 15, 1, 292, 1, 1, \ldots].$$

Pirmieji trys to skaičiaus reduktai yra

$$R_0=3, \quad R_1=\frac{22}{7}, \quad R_2=\frac{333}{106}.$$

Sudarysime (2.26) pavidalo skaičių aibę.

Kai $k=0$, turime 7 ($q_1=7$) skaičius:

$$\frac{4}{1}, \frac{7}{2}, \frac{10}{3}, \frac{13}{4}, \frac{16}{5}, \frac{19}{6}, \frac{22}{7}.$$

Kai $k=1$, turime 16 ($q_2+1=16$) skaičių:

$$\frac{3}{1}, \frac{25}{8}, \frac{47}{15}, \frac{69}{22}, \frac{91}{29}, \frac{113}{36}, \frac{135}{43}, \frac{157}{50}, \frac{179}{57}, \frac{201}{64}, \frac{223}{71},$$

$$\frac{245}{78}, \frac{267}{85}, \frac{289}{92}, \frac{311}{99}, \frac{333}{106}.$$

Išrinkę iš gautųjų skaičių tuos, kurių vardikiis ne didesnis už 60, o iš pastarųjų tuos, kurie yra arčiau skaičiaus negu bet kuri kita trupmena su ne mažesniu vardikliu, gauname šiuos geriausiuosius skaičiaus π artinius:

$$3, \frac{13}{4}, \frac{16}{5}, \frac{19}{5}, \frac{22}{7}, \frac{179}{57}.$$

Grandininėmis trupmenomis susidomėta po to, kai žinomas olandų fizikas, astronomas, matematikas *Hiuigensas* (Ch. Huygens, 1629–1695), bandydamas sukurti planetų judėjimo mechaninį modelį ir skaičiuodamas savo mechanizmo dantračių dantukų skaičius, susidūrė su reduktais – geriausiais artiniais. Sistemingą grandininių trupmenų teoriją kūrė *L. Oileris*, vėliau – *Ž. Lagranžas*.

Grandininės trupmenos plačiai taikomos. Pateiksime dar vieną pavyzdį. Pažymėkime α vidutinį parų skaičių astronominiuose metuose. Šis skaičius yra iracionalus:

$$\alpha=365{,}24220\ldots$$

Pirmieji α skleidinio grandinine trupmena elementai yra

$$\alpha = 365{,}24220\ldots = [365,\ 4,\ 7,\ 1,\ 3,\ \ldots], \tag{2.27}$$

o pirmieji to skleidinio reduktai –

$$R_0 = 365, \quad R_1 = 365\frac{1}{4}, \quad R_2 = 365\frac{7}{29}, \quad R_3 = 365\frac{8}{33}.$$

Jau senovės tautos žinojo reduktą $R_1 = 365\frac{1}{4}$. Juo buvo paremtas *Julijaus Cezario kalendorius*. Buvo laikoma, kad metus sudaro 365 ir $\frac{1}{4}$ paros, per 4 metus tos trupmeninės dalys sudarydavo vieną pilną parą. Taigi kas ketvirti metai (keliamieji metai) turėdavo 366 paras. Cezario kalendoriaus paklaida per 10 000 metų – 78 paros. XV a. tas kalendorius jau buvo atsilikęs nuo Saulės kalendoriaus 10 parų.

1589 m. kovo 1 d. popiežius *Grigalius XIII* išbraukė atsilikusias 10 parų ir nustatė, kad šimtmečiai, kurių pirmieji du skaitmenys sudaro iš 4 nesidalijantį dviženklį skaičių (pavyzdžiui, 1500 m.), nėra keliamieji metai. Tai reiškia, kad metai turi $365\frac{97}{400}$ parų. Ta reikšmė labai artima vienam iš geriausiųjų artinių, randamų pagal (2.26) formulę (kai $k = 3$, $x = 11$). Grigaliaus kalendoriaus paklaida – 3 paros per 10 000 metų.

Persų poetas ir matematikas *Omaras Chajamas* 1079 m. buvo sudaręs dar tikslesnį kalendorių. Tame kalendoriuje keliamieji buvo kas ketvirti metai 7 kartus, aštuntą kartą keliamieji buvo penkti metai. Per 33 metus susidarydavo 8 papildomos dienos. Tačiau šis santykis $\left(365\frac{8}{33}\right)$ yra ne kas kita kaip R_3. Chajamo kalendoriaus paklaida – 2 paros per 10 000 metų.

Uždaviniai

24. Įrodykite, kad du (2.26) pavidalo skaičiai, kuriuose x reikšmės skiriasi vienetu, tenkina 41 teoremos sąlygas.

25. Raskite skaičiaus e geriausius artinius, kurių vardikliai ne didesni už 50.

26. Raskite šių skaičių visus geriausius artinius:

a) $[-2, 1, 1, 4]$; b) $[3, 1, 1, 1, 2]$; c) $[4, 1, 1, 1, 1, 3]$.

27. Raskite skaičiaus α, aprašyto (2.27) lygybe, visus geriausius artinius, kurių vardikliai ne didesni už 50.

28. Raskite skaičių 13/29, 27/49 geriausius artinius, kurių vardikliai ne didesni už 20.

§24. Periodinės grandininės trupmenos

Priminsime, kad iracionaliojo skaičiaus α grandininė trupmena yra begalinė. Remiantis 20 paragrafe apibrėžta grandininės trupmenos liekanos sąvoka, bet kurią begalinę grandininę trupmeną galima užrašyti baigtiniu pavidalu:

$$\alpha = [q_0,\ q_1,\ q_2,\ \ldots\ q_{k-1},\ r_k].$$

Begalinė grandininė trupmena vadinama periodine, jei sutampa dvi skirtingų eilių liekanos.

Iš apibrėžimo išplaukia, kad periodinėms grandininėms trupmenoms galime rasti tokius sveikuosius skaičius k ir n, kad būtų

$$r_k = r_{k+n}. \tag{2.28}$$

Kadangi

$$r_k=[q_k,\ q_{k+1},\ \ldots,\ q_{k+n-1},\ r_{k+n}],$$

tai iš (2.28) lygybės išplaukia

$$q_{k+n}=q_k,$$

$$q_{k+n+1}=q_{k+1},$$

$$\ldots\ldots\ldots\ldots$$

$$q_{k+n+m}=q_{k+m};$$

čia m – bet koks natūrinis skaičius. Taigi periodinės grandininės trupmenos elementų seka, pradedant tam tikru numeriu, yra periodinė. Pastarąją savybę galima laikyti periodinės grandininės trupmenos apibrėžimu.

Jeigu grandininės trupmenos elementų seka yra periodinė pradedant jos pirmuoju elementu q_0, t. y. jeigu (2.28) lygybė teisinga, kai $k=0$, tai periodinė grandininė trupmena vadinama *grynąja periodine*, priešingu atveju – *mišriąja periodine grandinine trupmena.*

Pavyzdys. Grandininė trupmena

$$[7,\ 1,\ 1,\ 1,\ 7,\ 1,\ 1,\ 1,\ 7,\ 1,\ 1,\ 1,\ 7,\ \ldots]$$

yra grynoji periodinė, nes

$$r_0=r_4.$$

Grandininė trupmena

$$[-6,\ 1,\ 1,\ 2,\ 5,\ 9,\ 2,\ 5,\ 9,\ 2,\ 5,\ 9,\ \ldots]$$

yra mišrioji periodinė. Trys pirmieji jos elementai nesikartoja, periodą sudaro 3 elementai – 2, 5, 9. Šiuo atveju (2.28) lygybė yra

$$r_3=r_6.$$

Skaičius n, kurį apibrėžia (2.28) lygybė, vadinamas *periodo ilgiu.*

Jeigu periodinėje grandininėje trupmenoje α pirmasis periodo elementas yra q_{s+1}, o paskutinis – q_{s+n}, t. y.

$$\alpha=[q_0,\ q_1,\ \ldots,\ q_s,\ q_{s+1},\ \ldots,\ q_{s+n},\ q_{s+1},\ \ldots,\ q_{s+n},\ q_{s+1},\ \ldots],$$

tai ją sutrumpintai žymime

$$\alpha=[q_0,\ q_1,\ \ldots,\ q_s,\ \overline{q_{s+1},\ \ldots,\ q_{s+n}}].$$

Pavyzdžiai. 1. Išskleisime grandinine trupmena skaičių $-\sqrt{3}+1$.

$$[-\sqrt{3}+1]=-1,$$

$$-\sqrt{3}+1=-1+\frac{1}{\alpha_1},$$

$$\alpha_1=\frac{1}{-\sqrt{3}+2}=\frac{\sqrt{3}+2}{(-\sqrt{3}+2)(\sqrt{3}+2)}=\sqrt{3}+2=3+\frac{1}{\alpha_2},$$

$$\alpha_2=\frac{1}{\sqrt{3}-1}=\frac{\sqrt{3}+1}{2}=1+\frac{1}{\alpha_3},$$

$$\alpha_3=\frac{2}{\sqrt{3}-1}=\sqrt{3}+1=2+\frac{1}{\alpha_4},$$

$$\alpha_4=\frac{1}{\sqrt{3}-1}=\alpha_2,$$

Skaičiai α_i yra $-\sqrt{3}+1$ skleidinio grandinine trupmena liekanos r_i. Matome, kad liekanos r_2 ir r_4 sutampa. Taigi skaičių $-\sqrt{3}+1$ išskleidėme mišriąja periodine grandinine trupmena, kurios periodo ilgis lygus 2:

$$-\sqrt{3}+1=[-1, 3, 1, 2, 1, 2, 1, 2, \ldots]=[-1, 3, \overline{1, 2}].$$

2. Rasime skaičių α, aprašytą periodine grandinine trupmena

$$\alpha=[5, 1, \overline{3, 1, 2}].$$

Pagal grandininės trupmenos liekanos apibrėžimą

$$\alpha=[5, 1, r_2];$$

čia $r_2=[3, 1, 2, 3, 1, 2, \ldots]$.
Akivaizdu, kad

$$r_2=[3, 1, 2, r_2].$$

Grandininei trupmenai $[3, 1, 2, r_2]$ sudarome lentelę

	3	1	2	r_2
1	3	5	13	$13r_2+5$
0	1	1	3	$3r_2+1$

Grandininė trupmena $r_2=[3, 1, 2, r_2]$ sutampa su savo paskutiniu reduktu

$$r_2=\frac{13r_2+5}{3r_2+1}.$$

Sprendžiame kvadratinę lygtį

$$3r_2^2-12r_2-5=0.$$

Iš dviejų tos lygties šaknų imame tą, kurios sveikoji dalis lygi 3. Taigi

$$r_2=\frac{6+\sqrt{51}}{3}.$$

Tuomet skaičių α randame iš grandininės trupmenos

$$\alpha=[5, 1, r_2].$$

Taigi

$$\alpha=\frac{51+\sqrt{51}}{10}.$$

§25. Lagranžo teorema

Ankstesniame paragrafe išnagrinėti pavyzdžiai rodo, kad periodinės grandininės trupmenos susietos su kvadratinėmis iracionalybėmis – kvadratinių lygčių su sveikaisiais koeficientais šaknimis. Tas sąryšis nėra atsitiktinis. Prancūzų matematikas *Ž. Lagranžas* įrodė šią teoremą.

43 (Lagranžo) teorema. *Kiekviena kvadratinė iracionalybė yra išskleidžiama periodine grandinine trupmena.*

Įrodymas. Teoremą įrodinėsime keliais etapais.

1. Įrodysime, kad dviejų kvadratinių lygčių, kurių šaknys yra atitinkamai x ir y, diskriminantai lygūs, kai

$$x = m + \frac{1}{y}; \tag{2.29}$$

čia m – sveikasis skaičius.

Tarkime, kad

$$ax^2 + bx + c = 0. \tag{2.30}$$

Tos lygties diskriminantas yra

$$D_x = b^2 - 4ac.$$

Įrašę į (2.30) lygtį x reikšmę iš (2.29) lygybės, gauname

$$a\left(m + \frac{1}{y}\right)^2 + b\left(m + \frac{1}{y}\right) + c = 0,$$

arba

$$(am^2 + bm + c)\,y^2 + (2am + b)\,y + a = 0.$$

Iš čia

$$D_y = (2am + b)^2 - 4a\,(am^2 + bm + c) = b^2 - 4ac = D_x.$$

Kvadratinės lygties, kurios šaknis yra α, diskriminantą žymėsime D_α ir vadinsime α diskriminantu.

2. Įrodysime, kad kvadratinės iracionalybės skleidinio grandinine trupmena liekanų diskriminantai sutampa.

Kadangi

$$\alpha = [q_0,\ r_1] = q_0 + \frac{1}{r_1}$$

(q_0 – sveikasis skaičius) yra kvadratinė iracionalybė, tai ir r_1 yra kvadratinė iracionalybė. Taigi atitinkamų lygčių diskriminantai yra lygūs, t. y.

$$D_\alpha = D_{r_1}.$$

Kadangi bet kurios dvi skaičiaus α liekanos r_k ir r_{k+1} susietos lygybe

$$r_k = [q_k,\ r_{k+1}] = q_k + \frac{1}{r_{k+1}},$$

tai indukcijos metodu įsitikiname, kad visos skaičiaus α skleidinio grandinine trupmena liekanos yra kvadratinės iracionalybės ir atitinkamos lygtys turi tą patį diskriminantą D_α.

3. Naudodamiesi (2.13) formule, kvadratinę iracionalybę išreikšime liekana r_k:

$$\alpha = \frac{P_{k-1} r_k + P_{k-2}}{Q_{k-1} r_k + Q_{k-2}}. \tag{2.31}$$

Jeigu α yra lygties

$$Ax^2 + Bx + C = 0$$

šaknis, tai vietoj x įrašę skaičiaus α (2.31) išraišką įsitikiname, kad r_k yra kvadratinės lygties sprendinys:

$$A_k r_k^2 + B_k r_k + C_k = 0.$$

Tos lygties koeficientai yra

$$A_k = AP_{k-1}^2 + BP_{k-1}Q_{k-1} + CQ_{k-1}^2,$$

$$B_k = 2AP_{k-1}P_{k-2} + BP_{k-1}Q_{k-2} + BP_{k-2}Q_{k-1} + 2CQ_{k-1}Q_{k-2},$$

$$C_k = AP_{k-2}^2 + BP_{k-2}Q_{k-2} + CQ_{k-2}^2.$$

Taigi

$$C_k = A_{k-1}$$

ir

$$D_{r_k} = B_k^2 - 4A_k C_k = D_\alpha.$$

4. Šiuo etapu užbaigsime Lagranžo teoremos įrodymą. Iš (2.21) nelygybės išplaukia

$$\left| \alpha - \frac{P_{k-1}}{Q_{k-1}} \right| < \frac{1}{Q_{k-1}^2},$$

$$|P_{k-1} - \alpha Q_{k-1}| < \frac{1}{Q_{k-1}}. \tag{2.32}$$

(2.32) nelygybę galime užrašyti kaip lygybę

$$P_{k-1} - \alpha Q_{k-1} = \frac{\delta}{Q_{k-1}}; \tag{2.33}$$

čia δ – tam tikras realusis skaičius ir $|\delta| \leqslant 1$.

Iš (2.33) lygybės gautą skaičiaus P_{k-1} išraišką įrašę į koeficiento A_k išraišką, gauname

$$A_k = A\left(\alpha Q_{k-1} + \frac{\delta}{Q_{k-1}}\right)^2 + BQ_{k-1}\left(\alpha Q_{k-1} + \frac{\delta}{Q_{k-1}}\right) +$$

$$+ CQ_{k-1}^2 = Q_{k-1}^2 (A\alpha^2 + B\alpha + C) + 2A\alpha\delta + \frac{\delta^2}{Q_{k-1}^2} + B\delta.$$

Sklaustuose esantis reiškinys lygus 0, α yra lygties

$$Ax^2 + Bx + C = 0$$

šaknis. Todėl, kai $A>0$.

$$|A_k| \leqslant 2A|\alpha\delta| + \frac{A\delta^2}{Q_{k-1}^2} + |B\delta| \leqslant 2A|\alpha| + A + |B| = M.$$

Vadinasi, visų liekanų r_k lygčių vyriausiųjų koeficientų A_k moduliai ne didesni už pastovų skaičių M. Iš to išplaukia, kad koeficientai A_k gali įgyti tik baigtinį skaičių sveikųjų reikšmių. Ne daugiau sveikųjų reikšmių gali įgyti ir koeficientai C_k, nes

$$|C_k| = |A_{k-1}| \leqslant M.$$

Iš diskriminantų lygybės $B_k^2 - 4A_kC_k = B^2 - 4AC$ išplaukia

$$B_k^2 \leqslant 4|A_kC_k| + B^2 + 4A|C| \leqslant 4M^2 + B^2 + 4A|C| = N.$$

Taigi ir koeficientai B_k yra aprėžti pastovaus skaičiaus N, jie taip pat gali įgyti tik baigtinį skaičių skirtingų sveikųjų reikšmių.

Vadinasi, yra tik baigtinis skaičius skirtingų lygčių

$$A_kx^2 + B_kx + C_k = 0,$$

kurių šaknys — liekanos r_k. Tačiau kvadratinės iracionalybės α grandininė trupmena negali būti baigtinė (tuomet α būtų racionalusis skaičius). Skaičiaus α skleidinys grandinine trupmena turi be galo daug elementų q_k ir be galo daug liekanų r_k. Todėl yra liekanų, kurios tenkina tas pačias kvadratines lygtis, t. y. galima rasti tokius sveikuosius skaičius n ir k, kad būtų

$$r_k = r_{k+n}.$$

Atvirkščias teiginys įrodomas daug trumpiau.

44 teorema. *Bet kuri periodinė grandininė trupmena lygi kvadratinei iracionalybei.*

Įrodymas. Tarkime, kad skaičiaus α skleidinio grandinine trupmena liekanos r_k ir r_{k+n} sutampa. Remdamiesi 35 teorema, išreiškiame α:

$$\alpha = \frac{P_{k-1}r_k + P_{k-2}}{Q_{k-1}r_k + Q_{k-2}},$$

$$\alpha = \frac{P_{k+n-1}r_{k+n} + P_{k+n-2}}{Q_{k+n-1}r_{k+n} + Q_{k+n-2}}.$$

Sulyginę tų lygybių dešiniąsias puses, gauname kvadratinę lygtį $r_k = r_{k+n}$ atžvilgiu. Tos lygties šaknys negali būti racionalieji skaičiai, nes tuomet α būtų racionalus. O 30 teorema teigia, kad racionalieji skaičiai išskleidžiami baigtinėmis grandininėmis trupmenomis.

Nežinome dėsnių, nustatančių periodo ilgį. Pavyzdžiui,

$$\sqrt{5} = [2, \overline{4}], \quad \text{o} \quad \sqrt{1000} =$$

$$= [31, \overline{1, 1, 1, 1, 1, 6, 2, 2, 15, 2, 2, 6, 1, 1, 1, 1, 62}].$$

Uždaviniai

29. Išskleiskite grandinine trupmena šiuos skaičius:

$\sqrt{7}$, $2\sqrt{7}$, $3\sqrt{7}$, $4\sqrt{7}$, $1-\sqrt{8}$, $-\sqrt{13}$, $(\sqrt{5}+1)^{-1}$, $\sqrt{17}-7$, $\sqrt{a^2+1}$.

30. Raskite lygčių $x^3-3=0$, $x^3-4=0$, $x^3+x+1=0$, $x^3-x-1=0$, $x^4-2=0$ šaknų skleidinių grandinine trupmena po 5 elementus.

31. Raskite šiuos iracionaliuosius skaičius:

$$[\overline{1, 4}],\ [1, \overline{1, 2}],\ [1, \overline{1, 4}],\ [1, \overline{2, 3, 2}],\ [1, 4, \overline{5, 1}],$$

$$[1, 1, 3, \overline{1, 1, 2}],\ [\overline{a, b}],\ [a, b\ \overline{c}],\ [a, \overline{b, c}].$$

32. Raskite lygties, kurios šaknis yra $[a, \overline{b, c}]$, antrosios šaknies skleidinį grandinine trupmena.

33. Išskleiskite periodinėmis grandininėmis trupmenomis skaičius $\sqrt{3}$, $-\sqrt{2}$, $\sqrt{5}-5$, $\sqrt{6}$.

34. Raskite skaičių $[5, \overline{2, 3}]$, $-\sqrt{7}$, $(\sqrt{3}+1)^{-1}$ reduktus R_3, R_4, R_5, R_6 ir nustatykite, kokiu tikslumu jie išreiškia atitinkamus skaičius.

35. Trupmeną 2523/1762 pakeiskite mažesnio vardiklio trupmena, darydami paklaidą, ne didesnę už 10^{-4}.

§26. Grandininių trupmenų taikymai

Parodysime, kaip grandininės trupmenos taikomos pirmojo laipsnio neapibrėžtosioms lygtims su sveikaisiais koeficientais spręsti.

45 teorema. *Neapibrėžtosios lygties*

$$ax+by=c$$

su sveikaisiais koeficientais ir tarpusavyje pirminiais a ir $b>0$ *sveikasis sprendinys yra skaičių* x_0, y_0 *pora*:

$$x_0=(-1)^{k-1}c\cdot Q_{k-1},$$
$$y_0=(-1)^{k}c\cdot P_{k-1}; \tag{2.34}$$

čia P_{k-1} *ir* Q_{k-1} $(k>0)$ *— trupmenos* a/b *skleidinio priešpaskutinio redukto skaitiklis ir vardiklis.*

Įrodymas. Tarkime, kad $b>1$. Tada trupmena a/b turi daugiau kaip vieną reduktą ir todėl galima rasti jos priešpaskutinį reduktą.

Įrašysime į lygtį nurodytas x ir y reikšmes:

$$a(-1)^{k-1}cQ_{k-1}+b(-1)^{k}cP_{k-1}=c. \tag{2.35}$$

Jeigu $c=0$, ši lygybė teisinga. Jeigu $c\neq 0$,

$$aQ_{k-1}-bP_{k-1}=(-1)^{k-1}. \tag{2.36}$$

Žinome, kad bet kuris racionalusis skaičius a/b sutampa su savo skleidinio paskutiniu reduktu:

$$\frac{a}{b}=\frac{P_k}{Q_k}.$$

Abi tos trupmenos nesuprastinamos: pirmoji – pagal šios teoremos sąlygas, antroji – pagal 32 teoremos išvadą. Tuomet iš skaičiaus kanoninio skaidinio vienaties išplaukia

$$a=P_k, \quad b=Q_k.$$

Įrašę tas reikšmes į (2.36) lygybę, gauname tapatybę, kuri buvo įrodyta 32 teoremoje.

Jeigu $b=1$, tai lygties $ax+y=c$ sprendiniu galima imti skaičių porą $x_0=0$, $y_0=c$. Tačiau ir tos reikšmės sutampa su (2.34) formulėmis paėmus jose $k=0$, nes (2.4) lygybėmis sutarėme laikyti reikšmes $P_{-1}=1$, $Q_{-1}=0$.

Įrodėme, kad (2.34) formulėmis apibrėžtos x ir y reikšmės yra sveikieji lygties $ax+by=c$ sprendiniai su bet kuriuo sveikuoju neneigiamu k, kai $(a, b)=1$.

Baigdami nagrinėti pirmojo laipsnio dviejų kintamųjų Diofanto lygtį (t. y. lygtį, kurios ieškome tik sveikųjų sprendinių), suformuluosime teoremą apie tokios lygties sprendinių bendrąją išraišką.

46 teorema. *Jeigu* x_0, y_0 *yra lygties*

$$ax+by=c$$

sveikasis sprendinys, tai visi tos lygties sveikieji sprendiniai išreiškiami formulėmis

$$x=x_0+\frac{b}{(a, b)}\,t,$$

$$y=y_0-\frac{a}{(a, b)}\,t; \tag{2.37}$$

čia t *– bet koks sveikasis skaičius.*

Įrodymas. Priminsime, kad ši lygtis išsprendžiama tada ir tik tada, kai koeficientų a ir b didžiausias bendrasis daliklis (a, b) dalija laisvąjį narį c. Tuomet lygties

$$\frac{a}{(a, b)}\,x+\frac{b}{(a, b)}\,y=\frac{c}{(a, b)}$$

visi koeficientai yra sveikieji skaičiai, koeficientai prie kintamųjų – tarpusavyje pirminiai skaičiai. Teoremos įrodymas baigiamas pasirėmus 13 teorema.

9 paragrafe nagrinėjome pirmojo laipsnio lygčių su dviem kintamaisiais sprendimą taikant Euklido algoritmą ir Oilerio skliaustus. Iš tikrųjų tai tas pats sprendimo būdas, kurį pateikia ir 45 teorema. Jau minėjome, kad racionaliuosius skaičius galima skleisti grandinine trupmena naudojantis Euklido algoritmu. Kita vertus, šio paragrafo (2.3a) formulės rodo, kad reduktų skaitikliai ir vardikliai yra atitinkami Oilerio skliaustai.

Pavyzdžiai. 1. 9 paragrafe nagrinėjome (1.25) lygtį $23x-16y=6$. Skaičiaus 23/16 skleidinys grandinine trupmena yra [1, 2, 3, 2]. Trupmenos priešpaskutinis reduktas – 10/7. Priskirsime minuso ženklą, esantį prieš koeficientą 16, kintamajam y, t. y. rašysime $23x+$

$+16(-y)=6$. Taigi (2.34) formulėse reikia imti $k=3$, $P_{k-1}=10$, $Q_{k-1}=7$. Remdamiesi tomis formulėmis bei 46 teorema, randame minėtos lygties sprendinius:

$$x=42-16t, \quad y=60-23t.$$

Tuos pačius sprendinius buvome radę ir 9 paragrafe.

2. Ieškosime lygties

$$167x+39y=-2$$

sveikųjų sprendinių. Išskleisime skaičių 167/39 grandinine trupmena, naudodamiesi Euklido algoritmu:

$$167=39\cdot 4+11,$$

$$39=11\cdot 3+6,$$

$$11=6\cdot 1+5,$$

$$6=5\cdot 1+1,$$

$$5=1\cdot 5.$$

Taigi

$$\frac{167}{39}=[4,\ 3,\ 1,\ 1,\ 5].$$

Sudarysime lentelę reduktams skaičiuoti:

	$k=-1$	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$
q_k		4	3	1	1	5
P_k	1	4	13	17	30	167
Q_k	0	1	3	4	7	39

$k=4$ yra paskutinio redukto numeris. Priešpaskutinio redukto skaitiklis ir vardiklis yra $P_3=30$, $Q_3=7$. Iš (2.34) formulių gauname

$$x_0=-7\cdot(-2)=14,$$

$$y_0=30\cdot(-2)=-60.$$

Iš 46 teoremos išplaukia tokios sprendinių formulės:

$$x=14+39t, \quad y=-60-167t \quad (t\in\mathbf{Z}).$$

Grandininės trupmenos taikomos sprendžiant ir kitokias neapibrėžtąsias lygtis. Įrodyta, pavyzdžiui, kad

$$x^2-Dy^2=1$$

pavidalo neapibrėžtosios lygties, vadinamos *Pelio ir Ferma lygtimi*, sveikieji sprendiniai apskaičiuojami iš lygybių

$$x=P_{kn-1}, \quad y=Q_{kn-1}.$$

Tie skaičiai reiškia $\sqrt{D}$ skleidinio grandinine trupmena reduktų skaitiklius ir vardiklius. Skaičius k reiškia grandininės trupmenos periodo ilgį, be to,

sandauga kn turi būti lyginis skaičius, o D negali turėti daliklių, lygių sveikojo skaičiaus kvadratui.

Grandininėmis trupmenomis galima naudotis ieškant dviejų skaičių a ir b didžiausio bendrojo daliklio. Tam reikia skaičių a/b (arba b/a – tai nesvarbu) išskleisti grandinine trupmena. Radę paskutinį reduktą P_k/Q_k, kuris yra nesuprastinama trupmena, rasime $(a, b)=a/P_k$.

Naudojantis grandininėmis trupmenomis, randama ir skaičių a ir b didžiausio bendrojo daliklio d tiesinė išraiška. 6 teorema teigia, kad skaičių a ir b didžiausias bendrasis daliklis lygus tų skaičių Euklido algoritmo paskutinei nelygiai nuliui liekanai. Iš šios liekanos (1.9) išraiškos gauname

$$d=(-1)^{k-1}a\left((q_1, q_2, \ldots, q_{k-1})\right)+(-1)^k\times$$
$$\times b\left((q_0, q_1, q_2, \ldots, q_{k-1})\right);$$

čia k – trupmenos a/b skleidinio grandinine trupmena paskutinio redukto (arba elemento – tai tas pats) numeris, q_0 atitinka Euklido algoritmo (1.7) lygybėse vartotą žymėjimą q. Pasirėmę (2.3a) lygybėmis, d išraišką galime užrašyti trumpiau:

$$d=(-1)^{k-1}aQ_{k-1}+(-1)^k bP_{k-1}.$$

Padauginę abi šios lygybės puses iš c/d, gauname tapatybę, dar kartą įrodančią, kad (2.34) formulėmis apibrėžta skaičių x_0 ir y_0 pora yra lygties $ax+by=c$ sprendinys.

Uždaviniai

36. Naudodamiesi grandininėmis trupmenomis, raskite šių lygčių sveikuosius sprendinius:

$12x+13y=14$, $17x+19y=25$, $41x-14y=1$, $75x-18y=120$, $117x+17y=7$.

37. Naudodamiesi grandininėmis trupmenomis, raskite šių lygčių mažiausius natūrinius sprendinius:

$25x-y=4$, $17x-16y=1$, $82x-39y=10$.

38. Raskite skaičių a ir b didžiausio bendrojo daliklio tiesinę išraišką naudodamiesi grandininėmis trupmenomis:

1) $a=15$, $b=40$; 2) $a=62$, $b=100$; 3) $a=-24$, $b=96$; 4) $a=112$, $b=212$; 5) $a=300$, $b=75$.

39. Dviejų skaičių a ir b didžiausio bendrojo daliklio d tiesinė išraiška yra $d=-2a+3b$. Nustatykite bendrą išraišką skaičių a ir b, kurių d.b.d. turi tokią tiesinę išraišką.

40. Nustatykite skaičių a ir b išraiškas, kai jų d.b.d. yra šitokie:

$$d=-25a+17b, \quad d=36a-28b, \quad d=49a+50b.$$

41. *Fibonačio skaičiais* vadinami skaičiai

$$u_1, u_2, u_3, \ldots,$$

apibrėžiami rekurentine formule

$$u_1=1, \quad u_2=1,$$
$$u_n=u_{n-1}+u_{n-2} \quad (n\geqslant 3).$$

Kaip susiję Fibonačio skaičiai ir skaičiaus

$$\frac{\sqrt{5}+1}{2}$$

skleidinio reduktai?

Lyginiai

§27. Lyginio apibrėžimas. Pagrindinės lyginių savybės

Sveikųjų skaičių žiede **Z** apibrėšime naują sąryšį. Tarkime, kad m yra natūrinis skaičius.

Jeigu sveikųjų skaičių a ir b skirtumas $a-b$ dalijasi iš m, tai sakome, kad a lygsta b moduliu m ir rašome

$$a \equiv b \pmod{m}.$$

Šį reiškinį vadiname lyginiu (kongruencija).

Pavyzdžiui,

$$17 \equiv 2 \pmod{5},$$

$$-10 \equiv 24 \pmod{17}.$$

Jeigu skirtumas $a-b$ nesidalija iš m, tai sakome, kad *a nelygsta b moduliu m*. Tuo atveju rašome

$$a \not\equiv b \pmod{m}.$$

Pavyzdžiui,

$$13 \not\equiv 2 \pmod{6}.$$

Skaičius m lyginyje $a \equiv b \pmod{m}$ vadinamas *lyginio moduliu* (arba trumpiau — *moduliu*). Skaičiai a ir b vadinami *lyginio nariais*. (Jeigu $a \equiv b \pmod{m}$, dar sakoma, kad a ir b *kongruentūs* moduliu m.) Ženklas $\equiv$ vadinamas lyginio ženklu.

Atkreipsime dėmesį, kad lyginio apibrėžimu žodžiui „modulis“ suteikiama dar viena prasmė, skirtinga nuo jau žinomų kitų dviejų to žodžio prasmių (skaičiaus modulis — jo absoliutinis didumas, aibė modulis, apibrėžta § 6).

Kadangi bet kurių dviejų sveikųjų skaičių skirtumas visuomet dalijasi iš 1, tai lyginys $a \equiv b \pmod{1}$ jokios naujos informacijos neteikia. Todėl lyginio modulį laikysime didesniu už 1.

Aptarsime paprasčiausias lyginių savybes.

1. Refleksyvumo savybė. *Su kiekvienu sveikuoju skaičiumi a*

$$a \equiv a \pmod{m}.$$

Iš tikrųjų skirtumas $a-a=0$ dalijasi iš bet kurio natūrinio skaičiaus m.

2. Simetriškumo savybė. *Jeigu sveikuosius skaičius a ir b sieja lyginys*

$$a \equiv b \pmod{m},$$

tai

$$b \equiv a \pmod{m}.$$

Šią akivaizdžią savybę galime formuluoti ir šitaip: *lyginio narius galima sukeisti vietomis.*

3. Tranzityvumo savybė. *Jeigu sveikuosius skaičius a, b ir c sieja lyginiai*

$$a \equiv b \pmod{m}, \quad b \equiv c \pmod{m},$$

tai

$$a \equiv c \pmod{m}.$$

Iš tikrųjų, jeigu iš m dalijasi skirtumai $a-b$ ir $b-c$, tai iš m dalijasi ir tų skirtumų suma

$$(a-b)+(b-c)=a-c$$

Šiuo atveju galime sujungti lyginio ženklu keletą skaičių ir rašyti

$$a \equiv b \equiv c \pmod{m}.$$

Matematikos literatūroje galima rasti ir sutrumpintų lyginio užrašymo būdų, kuriuose praleistas ženklas mod arba ir visas simbolis (mod m) – tais atvejais, kai nekyla abejonių, kad kalbama apie lyginį, arba kai ilguose lyginių skaičiavimuose kartojasi tas pats modulis.

Jeigu skirtumas $a-b$ dalijasi iš m, tai tas skirtumas yra skaičiaus m kartotinis: $a-b=mt$ ($t \in \mathbf{Z}$). Todėl galime suformuluoti šitokią lyginių savybę.

4. Lyginio keitimas lygybe. *Sveikuosius skaičius a ir b sieja lyginys*

$$a \equiv b \pmod{m}$$

tada ir tik tada, kai egzistuoja toks sveikasis skaičius t, su kuriuo

$$a-b=mt.$$

5. Lyginių sudėtis. *Du lyginius tuo pačiu moduliu galima panariui sudėti: jeigu* $a \equiv b \pmod{m}$ *ir* $a' \equiv b' \pmod{m}$, *tai*

$$a+a' \equiv b+b' \pmod{m}.$$

Įrodymas. Pasirėmę 4 savybe, galime rasti sveikuosius skaičius t ir t', su kuriais būtų $a-b=mt$ ir $a'-b'=mt'$. Sudėję tas dvi lygybes, gauname lygybę $a+a'=b+b'+m(t+t')$, kuri ir reiškia, kad $a+a' \equiv b+b' \pmod{m}$.

6. Lyginių atimtis. *Du lyginius tuo pačiu moduliu galima panariui atimti: jeigu* $a \equiv b \pmod{m}$ *ir* $a' \equiv b' \pmod{m}$, *tai*

$$a-a' \equiv b-b' \pmod{m}.$$

Įrodoma panašiai kaip ir lyginių sudėtis.

7. Lyginių daugyba. *Du lyginius tuo pačiu moduliu galima panariui sudauginti: jeigu* $a \equiv b \pmod m$ *ir* $a' \equiv b' \pmod m$, *tai*

$$aa' \equiv bb' \pmod m.$$

Pasinaudoję 5 savybės įrodyme vartotais žymėjimais, gauname lygybę $aa' = (b+mt)(b'+mt') = bb' + m(bt' + b't + mtt')$, kuri ir rodo, kad aa' ir bb' lygsta moduliu m.

8. Narių perkėlimas. *Bet kurį lyginio narį galima perkelti į kitą lyginio pusę su priešingu ženklu: jeigu* $a \equiv b + c \pmod m$, *tai*

$$a - c \equiv b \pmod m.$$

Norint įrodyti šią savybę, pakanka prie lyginio $a \equiv b + c \pmod m$ pridėti visuomet teisingą lyginį $-c \equiv -c \pmod m$ ir remtis lyginių 1 bei 5 savybėmis.

9. Kėlimas laipsniu. *Lyginio abi puses galima kelti tuo pačiu natūriniu laipsniu: jeigu* $a \equiv b \pmod m$, *tai* $a^n \equiv b^n \pmod m$, $n \in \mathbf{N}$.

Ši savybė gaunama iš 7 savybės dauginant vienodus lyginius.

10. *Jeigu* $f(x)$ *yra polinomas su sveikaisiais koeficientais ir* $a \equiv b \pmod m$, ***tai***

$$f(a) \equiv f(b) \pmod m.$$

Įrodymas. Tarkime, kad $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. Jeigu $a \equiv b \pmod m$, tai, remdamiesi 9 savybe, gauname

$$a^2 \equiv b^2 \pmod m, \quad a^3 \equiv b^3 \pmod m, \ \ldots, \ a^n \equiv b^n \pmod m.$$

Iš 7 savybės išplaukia, kad bet kurį lyginį $a^r \equiv b^r \pmod m$ $(r = 0, \ldots, n)$ galime padauginti iš lyginio $a_r \equiv a_r \pmod m$. Tada

$$a_n a^n \equiv a_n b^n \pmod m, \quad a_{n-1} a^{n-1} \equiv a_{n-1} b^{n-1} \pmod m, \ \ldots,$$

$$a_1 a \equiv a_1 b \pmod m, \quad a_0 \equiv a_0 \pmod m.$$

Sudėję panariui šiuos lyginius, gauname

$$f(a) = a_n a^n + a_{n-1} a^{n-1} + \ldots + a_1 a + a_0 \equiv$$

$$\equiv a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 \pmod m.$$

Išnagrinėtosios lyginių savybės apima visus aritmetinius veiksmus, išskyrus dalybą. Dalyba yra kiek sudėtingesnis veiksmas, todėl jam skirsime atskirą teoremą.

47 teorema. *Jeigu d yra skaičių a ir b bendrasis daliklis, tai iš lyginio*

$$a \equiv b \pmod m$$

galima gauti lyginį

$$\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod} \ \frac{m}{(m, d)} \right). \tag{3.1}$$

Įrodymas. Pažymėkime raide g skaičių m ir d didžiausią bendrąjį daliklį. Tuomet egzistuoja tokie tarpusavyje pirminiai skaičiai (9 teorema) m_1 ir d_1, su kuriais teisingos lygybės

$$m=m_1 g, \quad d=d_1 g.$$

Kadangi d yra skaičių a ir b bendrasis daliklis (nebūtinai didžiausias), tai galima rasti skaičius a_1 ir b_1, su kuriais būtų teisingos lygybės

$$a=a_1 d, \quad b=b_1 d.$$

Remiantis 4 savybe, lyginį $a\equiv b \pmod m$ galima pakeisti lygybe $a-b=mt$, t. y.

$$a_1 d_1 g - b_1 d_1 g = m_1 g t.$$

Padaliję šios lygybės narius iš g, gauname

$$a_1 d_1 - b_1 d_1 = m_1 t.$$

Pastarosios lygybės kairioji pusė dalijasi iš d_1. Vadinasi, iš to skaičiaus dalijasi ir dešinioji pusė — sandauga $m_1 t$. Tačiau, kaip minėjome, skaičiai m_1 ir d_1 yra tarpusavyje pirminiai. Todėl iš d_1 turi dalytis skaičius t. Taigi $t=d_1 t_1$. Įrašę šią t išraišką į nagrinėjamąją lygybę ir suprastinę iš d_1, gauname

$$a_1 - b_1 = m_1 t_1.$$

Nesunku įsitikinti, kad iš šios lygybės išplaukia (3.1) lyginys. Teorema įrodyta.

Išvada. *Jeigu skaičių a ir b bendrasis daliklis d ir modulis m yra tarpusavyje pirminiai, tai lyginio $a\equiv b \pmod m$ abi puses galima padalyti iš to daliklio (nekeičiant modulio):*

$$\frac{a}{d}\equiv\frac{b}{d} \pmod m.$$

Teiginys išplaukia iš (3.1) lygybės, nes $(m, d)=1$.

Visos nagrinėtosios lyginių savybės analogiškos atitinkamoms lygybių savybėms: lyginius, kaip ir lygybes, galima panariui sudėti, atimti, sudauginti, lyginio narius galima kelti iš vienos lyginio pusės į kitą su priešingu ženklu, abi lyginio puses galima dauginti iš to paties sveikojo skaičiaus, jas kelti bet kuriuo natūriniu laipsniu. Lyginio narių dalybą iš sveikojo skaičiaus apibūdina 47 teorema ir jos išvada.

Iš lyginių 5 savybės išplaukia viena neįprasta taisyklė, kuriai analogiškos nėra tarp lygybių savybių: *prie (iš) bet kurios lyginio pusės galima pridėti (atimti) bet kurį modulio kartotinį, t. y. jeigu $a\equiv b \pmod m$, tai*

$$a\equiv b+mt \pmod m$$

ir atvirkščiai. Įrodymas paprastas: prie lyginio $a\equiv b \pmod m$ panariui pridedame lyginį $0\equiv mt \pmod m$, kuris, be abejo, visada teisingas ($t\in\mathbf{Z}$). Ši taisyklė leidžia supaprastinti lyginį sumažinant visus jo koeficientus, jei jų moduliai didesni už m.

Pavyzdžiui, lyginį

$$372-415a—707a^3-1411b \pmod 7$$

pakeisime paprastesniu prie jo kairiosios pusės pridėję modulio 7 kartotinį $7\cdot 101a^3$:

$$372-415a\equiv 1411b \pmod 7.$$

Iš šio lyginio dešiniosios pusės atėmę modulio kartotinį $7\cdot 201b$, gausime

$$372-415a\equiv 4b \pmod 7.$$

Analogiškai prastindami toliau, galime gauti lyginį

$$1-2a\equiv 4b \pmod 7.$$

Galima sumažinti koeficientus ir prie a bei b. Pridėję prie lyginio kairiosios pusės modulio kartotinį 7 ir po to, remdamiesi 47 teoremos išvada, padaliję visus lyginio narius iš 2, gausime

$$4-a\equiv 2b \pmod 7.$$

Šio lyginio išraišką galime ir toliau panašiai keisti.

Pavyzdžiai. 1. Sudėję, atėmę ir sudauginę panariui lyginius

$$13\equiv 1 \pmod 6 \quad \text{ir} \quad 5\equiv -7 \pmod 6,$$

gausime jų

sumą: $18\equiv -6 \pmod 6$,

skirtumą: $8\equiv 8 \pmod 6$,

sandaugą: $65\equiv -7 \pmod 6$.

2. Lyginio $4\equiv -2 \pmod 6$ abi puses padauginę iš 5, pakėlę kvadratu ir kubu, gausime to lyginio

5 kartotinį: $20\equiv -10 \pmod 6$,

kvadratą: $16\equiv 4 \pmod 6$,

kubą: $64\equiv -8 \pmod 6$.

3. Imkime $f(x)=x^2-3x+1$. Patikrinsime lyginių 10 savybę šiam polinomui bei lyginiui $5\equiv -7 \pmod 6$. Randame

$$f(5)=11, \quad f(-7)=71.$$

Kadangi $11\equiv 71 \pmod 6$, tai

$$f(5)\equiv f(-7) \pmod 6.$$

4. Suprastinsime lyginį

$$180a\equiv 285 \pmod{213}.$$

Kadangi $(180, 285)=15$, o $(15, 213)=3$, tai pagal 47 teoremą

$$\frac{180a}{15}\equiv\frac{285}{15}\left(\text{mod }\frac{213}{3}\right),$$

arba

$$12a\equiv 19 \pmod{71}.$$

5. Suprastinkime lyginį

$$96 \equiv 132x \pmod{41},$$

Randame $(96, 132)=12$, $(12, 41)=1$. Šiuo atveju remiamės 47 teoremos išvada ir gauname lyginį

$$8 \equiv 11x \pmod{41}.$$

6. Jeigu abi lyginio puses dalydami iš bendrojo daliklio neatsižvelgsime į modulį, tai galime gauti neteisingą rezultatą. Pavyzdžiui, padaliję lyginio

$$56 \equiv 40 \pmod{16}$$

abi puses iš 8 ir palikę modulį nepakeistą, gautume teiginį

$$7 \equiv 5 \pmod{16},$$

kuris jau nėra teisingas, nes $7-5=2$ nesidalija iš 16. Taigi

$$7 \not\equiv 5 \pmod{16}.$$

Uždaviniai

1. Kurie iš šių skaičių lygsta vienas kitam moduliu 7:

$$2, -64, 36, -3, 7000, 17, 23, 13, 5, 143, -14, 12, 32?$$

2. Raskite t reikšmes, su kuriomis šios skaičių poros lygsta moduliu 11:

1) $2t$, $t+4$; 2) $5t-1$, $-5t+2$; 3) $3t$, $t-100$;
4) $3t-8$, $t+11$; 5) $11t+7$, $11t-4$.

3. Nustatykite, kokiais moduliais lygsta šios skaičių poros:

1) -74 ir 16; 2) 105 ir -105; 3) -1 ir 199; 4) $17a$ ir $-a$.

4. Suprastinkite lyginius:

1) $128 \equiv -64 \pmod{13}$;
2) $128 \equiv -64 \pmod{12}$;
3) $180 \equiv 27 \pmod{17}$;
4) $225 \equiv 750 \pmod{35}$;
5) $1440 \equiv 96 \pmod{84}$;
6) $40^{10} \equiv 25^{20} \pmod{45^{15}}$.

5. Suprastinkite lyginius:

1) $137x \equiv 14 \pmod{15}$; 2) $65x^3-26x^2-40x \equiv 100 \pmod{13}$;
3) $144x^2-100x+20 \equiv 17 \pmod{12}$; 4) $39x-75 \equiv 75-39x \pmod{18}$;

čia x – sveikasis skaičius.

§28. Liekanų (likinių) klasės. Liekanų klasių žiedas

Lyginio sąvoka apibrėžia naują sąryšį sveikųjų skaičių aibėje. Praeitame paragrafe matėme, kad sąryšis „lygsta moduliu m“ yra refleksyvus, simetrinis ir tranzityvus. Kaip jau žinome (žr. vadovėlio I d.), tokie sąryšiai savo apibrėžimo aibę suskirsto į nesikertančias ekvivalentumo klases. Dabar ir nagrinėsime tas klases.

Nagrinėdami ekvivalentumo klases, buvome sutarę, kad vienai klasei priklauso visi tie aibės elementai, kurie susieti ekvivalentumo sąryšiu.

Ekvivalentumo klasei sąryšio „lygsta moduliu m“ atžvilgiu (kad būtų trumpiau, toliau vadinsime „ekvivalentumo klase moduliu m“) priklauso visi tie sveikieji skaičiai, kurie lygsta vienas kitam moduliu m. Jeigu, pavyz-

džiui, vienai klasei šio sąryšio atžvilgiu priklauso skaičiai a, b, c, d, ..., tai

$$a \equiv b \pmod{m},$$

$$b \equiv c \pmod{m},$$

$$c \equiv d \pmod{m}$$

ir t. t., arba trumpiau

$$a \equiv b \equiv c \equiv d \equiv \ldots \pmod{m}.$$

Taigi vieną ekvivalentumo klasę (trumpiau – klasę) moduliu m sudaro tie ir tik tie sveikieji skaičiai, kurie lygsta vienas kitam tuo moduliu.

Jeigu klasei moduliu m priklauso skaičius a, tai bet kuris kitas tos klasės skaičius x su skaičiumi a susietas lyginiu

$$x \equiv a \pmod{m}.$$

Praeitame paragrafe jau aptarėme, kad tas lyginys gali būti pakeičiamas lygybe

$$x = a + mt \quad (t \in \mathbf{Z}). \tag{3.2}$$

Vadinasi, ekvivalentumo klasę moduliu m galima nusakyti šitaip: jeigu klasei priklauso skaičius a, tai visi tos klasės skaičiai x yra (3.2) pavidalo. Tą klasę galima būtų žymėti K_a. Šis žymėjimas nevienareikšmis – skaičius a yra laisvai pasirinktas klasės elementas. Vietoje a paėmę kitą klasės elementą b, tą pačią klasę galime žymėti K_b. Visus galimus vienos ir tos pačios klasės žymėjimus galime apibūdinti šitaip:

$$K_a = K_b, \quad \text{kai} \quad a \equiv b \pmod{m}.$$

Reikia rasti kiekvienos ekvivalentumo klasės moduliu m vienareikšmį žymėjimo būdą ir kartu nustatyti galimą klasių skaičių. Tuo tikslu įrodysime šitokią teoremą.

48 teorema. *Du sveikieji skaičiai lygsta vienas kitam moduliu m tada ir tik tada, kai dalijant juos iš m gaunama ta pati liekana.*

Įrodymas. Remdamiesi dalybos su liekana teorema, užrašykime lygybes

$$a = mq + r,$$

$$b = mq' + r',$$

kuriose liekanos r ir r' yra neneigiamos ir mažesnės už m.

Teoremos sąlygos pakankamumas akivaizdus: jeigu $r = r'$, tai

$$a - b = m(q - q'),$$

ir todėl $a \equiv b \pmod{m}$.

Įrodysime sąlygos būtinumą. Tarkime, kad $r \geqslant r'$. Tada

$$a - b = m(q - q') + r - r'. \tag{3.3}$$

Jeigu $a \equiv b \pmod{m}$, tai skirtumas $a-b$ dalijasi iš m. Tuomet (3.3) lygybėje skirtumas $r-r'$ taip pat turi dalytis iš m:

$$r-r'=ms.$$

Tačiau minėjome, kad liekanos r ir r' mažesnės už m. Šis skirtumas pagal prielaidą neneigiamas. Todėl pastaroji lygybė galima tik tada, kai $r=r'$. Teorema įrodyta.

Ši teorema rodo, jog visi skaičiai, kurie lygsta vienas kitam moduliu m, pasižymi tuo, kad juos dalijant iš m gaunama viena ir ta pati neneigiama liekana r. Todėl ir ekvivalentumo klasę sąryšio „lygsta moduliu m“ atžvilgiu galime pavadinti vienodas liekanas (gautas dalijant iš m) turinčių skaičių klase, arba *vienodų liekanų klase moduliu m*. Trumpumo dėlei žodį „vienodų“ praleidžiame ir kalbame apie liekanų klases pasirinktuoju moduliu. Beje, kiti autoriai siūlo vartoti terminą „likinių klasė“.

Kadangi visos galimos neneigiamos liekanos, kurios gaunamos sveikuosius skaičius dalijant iš m, yra

$$0,\ 1,\ 2,\ \ldots,\ m-1,$$

tai yra lygiai m liekanų klasių moduliu m. Kiekvienai klasei atstovauja viena ir tik viena liekana, gaunama bet kurį tos klasės skaičių dalijant iš m. Taigi liekanų klases galime žymėti ir šitaip:

$$K_0,\ K_1,\ K_2,\ \ldots,\ K_{m-1}.$$

Tokį žymėjimą vadinsime *standartiniu*, tuo jį atskirdami nuo anksčiau minėto žymėjimo K_a (a – bet kuris liekanų klasės skaičius). Vartosime abu žymėjimus – kiekvienas jų turi savo privalumų, taip pat ir trūkumų.

Liekanų (likinių) klasę moduliu m sudaro visi sveikieji skaičiai, kurie lygsta vienas kitam moduliu m.

Liekanų klasę žymėsime K_a; čia a – bet kuris tos klasės skaičius.

Iš anksčiau pateiktų pastabų išplaukia, kad šiam apibrėžimui ekvivalentus toks apibrėžimas.

Liekanų (likinių) klasę K_a moduliu m sudaro visi

$$a+mt, \quad t \in \mathbf{Z},$$

pavidalo sveikieji skaičiai.

Pavyzdžiai. 1. Skaičiai 10, -4, -11, 73, 3 lygsta vienas kitam moduliu 7. Iš tikrųjų

$$10 \equiv -4 \pmod{7}$$

$$-4 \equiv 73 \pmod{7},$$

$$73 \equiv 3 \pmod{7}$$

ir t. t. Taigi šie skaičiai priklauso tai pačiai liekanų klasei moduliu 7, kurią galime įvairiai žymėti:

$$K_{10}=K_{-4}=K_{-11}=K_{73}$$

ir t. t. Patikrinsime, ar minėtuosius šios klasės skaičius dalijant iš 7 visada gaunama ta pati liekana:

$$10=7\cdot 1+3,$$

$$-4=7\cdot(-1)+3,$$

$$-11=7\cdot(-2)+3,$$

$$73=7\cdot 10+3.$$

Visų šių skaičių liekana, dalijant juos iš 7, lygi 3. Liekanų klasės standartinis žymėjimas yra K_3.

2. Pirmajame pavyzdyje įsitikinome, kad skaičiai 10, -4, -11, 73 priklauso liekanų klasei K_3 moduliu 7. Remdamiesi antruoju liekanų klasės apibrėžimu, galime užrašyti šitokias bet kurio tos liekanų klasės elemento x išraiškas:

$$x=10+7t_1,$$

$$x=-4+7t_2,$$

$$x=-11+7t_3,$$

$$x=73+7t_4$$

ir t. t.; čia $t_i\in\mathbf{Z}$. Iš standartinio liekanų klasės K_3 žymėjimo išplaukia šitokia to paties elemento x išraiška:

$$x=3+7t \quad (t\in\mathbf{Z}).$$

3. Sveikieji skaičiai -2, 11, -19, 100 priklauso ne tai pačiai liekanų klasei moduliu 13. Pirmieji du skaičiai lygsta moduliu 13 ir priklauso liekanų klasei K_{11} tuo moduliu. Kiti du skaičiai priklauso kitoms dviem liekanų klasėms moduliu 13, būtent, $-19\in K_7$, o $100\in K_9$, nes

$$-19\equiv 7 \pmod{13},$$

$$100\equiv 9 \pmod{13}.$$

Iki šiol vartotų liekanų klasių žymėjimų trūkumas tas, kad nenurodomas modulis. Liekanų klasė K_3 moduliu 7 ir liekanų klasė K_3 moduliu 8 vienodai žymimos, bet skirtingos aibės, nors kai kurie jų elementai gali ir sutapti. Todėl reikia atsiminti, kokiu moduliu apibrėžtos liekanų klasės.

Liekanų klasę galima užrašyti kaip aibę, kurios elementai žinomi.

Jeigu $r\in\{0, 1, 2, \ldots, m-1\}$, tai

$$K_r=\{b \mid b\equiv r \pmod m\}=\{r+mt \mid t\in\mathbf{Z}\}.$$

Visa sveikųjų skaičių aibė $\mathbf{Z}$ skirstoma į m nesikertančių liekanų klasių moduliu m:

$$\mathbf{Z}=K_0\cup K_1\cup\ldots\cup K_{m-1}.$$

Pažymėkime sveikųjų skaičių aibės $\mathbf{Z}$ faktoraibę pagal sąryšį „lygsta moduliu m“ simboliu $\mathbf{Z}/(m)$:

$$\mathbf{Z}/(m)=\{K_0, K_1, \ldots, K_{m-1}\}.$$

Šią aibę vadinsime *liekanų klasių moduliu m aibe.*

Pavyzdys. Kai $m=5$,

$$K_0=\{5t \mid t\in\mathbf{Z}\},\quad K_1=\{5t+1 \mid t\in\mathbf{Z}\},\quad K_2=\{5t+2 \mid t\in\mathbf{Z}\},$$

$$K_3=\{5t+3 \mid t\in\mathbf{Z}\},\quad K_4=\{5t+4 \mid t\in\mathbf{Z}\};$$

$$\mathbf{Z}=K_0\cup K_1\cup K_2\cup K_3\cup K_4.$$

Liekanų klasių aibių galima sudaryti be galo daug – kiekvieną modulį m atitinka liekanų klasių moduliu m aibė.

Liekanų klasių moduliu m aibėje apibrėšime veiksmus – liekanų klasių sudėtį ir daugybą:

$$K_a+K_b=K_{a+b},$$

$$K_a\cdot K_b=K_{ab}.$$

Apibrėžę veiksmus liekanų klasių moduliu m aibėje, gauname algebrinę struktūrą, kurią žymėsime L_m:

$$L_m=(\mathbf{Z}/(m),\ +,\ \cdot).$$

Iš veiksmų apibrėžimo išplaukia, kad, sudedant ar sudauginant dvi liekanų klases, sudedami ar sudauginami atitinkami sveikieji skaičiai a ir b. Tačiau sveikųjų skaičių suma ir sandauga randamos vienareikšmiškai. Sudėtis ir daugyba sveikųjų skaičių aibėje yra komutatyvios, asociatyvios ir tarpusavyje distributyvios operacijos, todėl tokiomis pat savybėmis pasižymi ir liekanų klasių sudėtis bei daugyba. Nesunku įsitikinti, kad liekanų klasės K_0 ir K_1 yra atitinkamai nulinis ir vienetinis elementai liekanų klasių moduliu m aibėje apibrėžtų operacijų atžvilgiu. Iš tikrųjų

$$K_a+K_0=K_{a+0}=K_a,$$

$$K_a\cdot K_1=K_{a\cdot 1}=K_a,$$

$$K_a\cdot K_0=K_{a\cdot 0}=K_0.$$

Visai taip pat galima įsitikinti, kad liekanų klasė K_{-a} yra liekanų klasei K_a priešingas elementas sudėties operacijos atžvilgiu.

Iš šių pastabų išplaukia, kad *struktūra L_m yra komutatyvusis žiedas su vienetiniu elementu.*

Pavyzdys. Atliksime keletą veiksmų su liekanų klasėmis moduliu 7:

$$K_{12}+K_{22}=K_{34},\qquad K_{10}+K_{-8}=K_2,$$

$$K_{13}-K_{-3}=K_{16},\qquad K_{11}\cdot K_5=K_{55},$$

$$K_6\cdot K_5=K_{30},$$

Veiksmų su liekanų klasėmis moduliu m taisyklės labai paprastos, jas lengva įsiminti, tačiau jos nesiderina su standartiniu liekanų klasių žymėjimu

(tai akivaizdu iš paskutinio pavyzdžio). Norėdami aprašyti veiksmus su standartiškai pažymėtomis liekanų klasėmis moduliu m, galime sudaryti pagalbines sudėties ir daugybos lenteles.

Liekanų klasių moduliu 6, pažymėtų standartiškai, daugybos lentelė yra šitokia:

	K_0	K_1	K_2	K_3	K_4	K_5
K_0	K_0	K_0	K_0	K_0	K_0	K_0
K_1	K_0	K_1	K_2	K_3	K_4	K_5
K_2	K_0	K_2	K_4	K_0	K_2	K_4
K_3	K_0	K_3	K_0	K_3	K_0	K_3
K_4	K_0	K_4	K_2	K_0	K_4	K_2
K_5	K_0	K_5	K_4	K_3	K_2	K_1

Pavyzdžiui, šios lentelės trečiosios eilutės, pažymėtos K_2, ir penktojo stulpelio, pažymėto K_4, sankirtoje yra klasė K_2, lygi klasių K_2 ir K_4 sandaugai. Iš tikrųjų

$$K_2 \cdot K_4 = K_8 = K_2.$$

Nagrinėdami liekanų klasių moduliu 6 daugybos lentelę, pastebime vieną sveikųjų skaičių daugybai nebūdingą savybę — dviejų nenulinių šio žiedo elementų K_2 ir K_3 sandauga yra nulinis elementas — liekanų klasė K_0.

Žiedas, kurio nenulinių elementų sandauga yra nulinis elementas, vadinamas *žiedu su nulio dalikliais*, o tokie jo elementai vadinami *nulio dalikliais*.

Uždaviniai

6. Įrodykite: jeigu modulis yra sudėtinis skaičius, tai liekanų klasių tuo moduliu žiedas turi nulio daliklių.

7. Nurodykite, kokioms liekanų klasėms priklauso skaičiai -14, 11, -13, -2, -1, 0, 3, 7, 18, 21, 25, 49, 81, 100, kai:

1) $m=7$; 2) $m=11$; 3) $m=13$; 4) $m=12$.

8. Nurodykite, kokioms liekanų klasėms priklauso skaičiai a, $-20<a<20$, kai:

1) $m=8$; 2) $m=9$; 3) $m=11$; 4) $m=12$.

9. Užrašykite visus dviženklius skaičius, priklausančius liekanų klasei K_{13} moduliu m, kai:

1) $m=14$; 2) $m=15$; 3) $m=16$; 4) $m=17$.

10. Nustatykite, su kuria a reikšme skaičiai $7a-12$ ir $a+5$ priklauso tai pačiai liekanų klasei moduliu m, kai:

1) $m=7$; 2) $m=6$; 3) $m=9$; 4) $m=11$.

11. Sudarykite liekanų klasių moduliu m sudėties ir daugybos lenteles, kai:

1) $m=5$; 2) $m=7$; 3) $m=8$; 4) $m=9$.

12. Atlikite veiksmus su liekanų klasėmis moduliu m

K_3+K_{97}, K_2-K_{20}, $K_6 \cdot K_7 \cdot K_8 \cdot K_9$, $(K_{10})^{10}$, kai modulis yra:

1) $m=13$; 2) $m=11$; 3) $m=17$; 4) $m=12$.

13. Raskite liekanų klasės K_0 moduliu 7 ir liekanų klasės K_0 moduliu 11 sankirtą.

14. Išspręskite liekanų klasių moduliu 13 aibėje lygtis

$$K_x \cdot K_a = K_1$$

su kiekvienu a, $0<a\leqslant 12$.

§29. Liekanų sistemos moduliu m

Apibrėšime dvi liekanų sistemas – *pilnąją* ir *redukuotąją*.

Pilnoji liekanų sistema.

Rinkinys skaičių, paimtų po vieną iš kiekvienos liekanų klasės moduliu m, vadinamas pilnąja liekanų sistema tuo moduliu.

Pilnoji liekanų sistema (sutrumpintai p. l. s.) moduliu m turi m elementų – po vieną iš visų m liekanų klasių moduliu m.

Pavyzdžiui, aibė $-10, 11, 12, -2, -11$ yra pilnoji liekanų sistema moduliu 5. Iš tikrųjų šie skaičiai atstovauja visoms liekanų klasėms tuo moduliu:

klasei K_0 – skaičius -10,
„ K_1 „ 11,
„ K_2 „ 12,
„ K_3 „ -2,
„ K_4 „ -11.

Štai dar kelios pilnosios liekanų sistemos moduliu 5:

$0, -4, -8, 3, 9,$
$0, 1, 2, 3, 4,$
$0, 1, 2, -2, -1.$

Suformuluosime pilnosios liekanų sistemos sudarymo kriterijų.

Kad sveikieji skaičiai sudarytų pilnąją liekanų sistemą moduliu m, būtina ir pakankama, kad jų būtų m ir bet kurie du iš jų nelygtų vienas kitam moduliu m.

Iš tikrųjų, kai ta sąlyga išpildoma, skaičiai atstovauja visoms liekanų klasėms moduliu m.

Pavyzdžiai. 1. Nustatysime, ar skaičiai 148, -37, 501, 102, 804 sudaro p. l. s. moduliu 5.

Kadangi

$$148 \equiv -37 \pmod 5,$$

tai tie skaičiai nesudaro p. l. s. moduliu 5.

2. Nustatysime, ar skaičiai 4, 11, 0, -11, 80, 1 sudaro p. l. s. moduliu 7.

Pilnoji liekanų sistema moduliu 7 turi turėti 7 skaičius, o čia jų tik 6. Jokie 6 skaičiai negali sudaryti p. l. s. moduliu 7.

Kartais patogu p. l. s. parinkti specialiu būdu. Nurodysime du tokius parinkimo būdus.

Galime sudaryti p. l. s. moduliu m parinkdami liekanų klasėse mažiausius neneigiamus skaičius – standartinio žymėjimo numerius:

$$0, 1, 2, \ldots, m-1.$$

Tokią liekanų sistemą vadiname *mažiausių neneigiamų liekanų sistema moduliu m.*

Kita speciali sistema yra *mažiausių teigiamų liekanų sistema moduliu m*:

$$1, 2, \ldots, m.$$

Dar vienas būdas p. l. s. sudaryti yra absoliutiniu didumu mažiausių skaičių iš liekanų klasių moduliu m išrinkimas. Kai m – nelyginis skaičius, absoliutiniu didumu mažiausių atstovų iš klasių rinkinį sudarys skaičiai

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}.$$

Kai modulis – lyginis skaičius, tokią sistemą galima sudaryti dviem būdais:

$$-\frac{m}{2}, -\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1,$$

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1, \frac{m}{2}.$$

Šio pavidalo sistemos vadinamos *absoliutiniu didumu mažiausių liekanų sistemomis.*

Pavyzdžiui, sudarysime mažiausių neneigiamų ir absoliutiniu didumu mažiausių liekanų sistemas moduliais 5 ir 6.

Moduliu 5: a) 0, 1, 2, 3, 4,
b) −2, −1, 0, 1, 2;
moduliu 6: a) 0, 1, 2, 3, 4, 5,
b) −3, −2, −1, 0, 1, 2

arba

−2, −1, 0, 1, 2, 3.

Įrodysime teoremą apie p. l. s. transformacijas.

49 teorema. *Jeigu x įgyja visas pilnosios liekanų sistemos moduliu m elementų reikšmes, tai ir*

$$ax+k$$

pavidalo skaičiai taip pat sudaro pilnąją liekanų sistemą tuo pačiu moduliu, kai $(a, m)=1$.

Įrodymas. Tarkime, kad x įgyja visas reikšmes šios p. l. s. moduliu m:

$$d_1, d_2, \ldots, d_m.$$

Įrodysime, kad tuomet skaičiai

$$ad_1+k, \quad ad_2+k, \quad \ldots, \quad ad_m+k$$

taip pat sudaro p. l. s. moduliu m. Iš tikrųjų naujai sudarytų skaičių taip pat yra m. Reikia įsitikinti, kad jie poromis nelygsta vienas kitam moduliu m. Iš bet kurio lyginio

$$ad_i+k \equiv ad_j+k \pmod m,$$

$$1 \leqslant i, \quad j \leqslant m,$$

remdamiesi operacijų su lyginiais savybėmis ir tuo, kad $(a, m)=1$, gautume šitokį lyginį

$$d_i \equiv d_j \pmod{m}.$$

Tas lyginys neteisingas, kai $i \neq j$, o skaičiai $d_1, d_2, \ldots, d_m$ sudaro p. l. s. moduliu m.

Pavyzdys. Matėme, kad skaičiai $-2, -1, 0, 1, 2$ sudaro p. l. s. moduliu 5. Transformuosime tą sistemą imdami $a=-1$, $k=2$. Gausime skaičius

$$4, 3, 2, 1, 0,$$

kurie sudaro p. l. s. moduliu 5.

Redukuotoji liekanų sistema. Nagrinėdami kelių skaičių didžiausią bendrąjį daliklį, 7 paragrafe įrodėme šią jo savybę:

$$a=bq+r \Rightarrow (a, b)=(b, r).$$

Iš tos savybės išplaukia, kad visų vienos liekanų klasės moduliu m skaičių ir modulio m didžiausias bendrasis daliklis yra tas pats skaičius.

Iš tikrųjų, jeigu $a, b \in K_a$ moduliu m, tai

$$a \equiv b \pmod{m}$$

ir

$$a=b+mt.$$

Iš minėtosios d. b. d. savybės išplaukia, kad

$$(a, m)=(b, m).$$

Liekanų klasės K_a moduliu m ir to modulio didžiausią bendrąjį daliklį apibrėšime lygybe

$$(K_a, m)=(a, m).$$

Liekanų klasė K_a moduliu m vadinama tarpusavyje pirmine su tuo moduliu, jei $(a, m)=1$.

Pavyzdžiui, moduliu 6 yra tik dvi su moduliu tarpusavyje pirminės klasės — K_1 ir K_5.

Rinkinys skaičių, paimtų po vieną iš kiekvienos liekanų klasės, tarpusavyje pirminės su moduliu m, vadinamas redukuotąja liekanų sistema moduliu m.

Paprastas būdas redukuotajai liekanų sistemai (sutrumpintai r. l. s.) moduliu m sudaryti — reikia imti pilnąją liekanų sistemą tuo moduliu ir iš

jos išbraukti tuos skaičius, kurie nėra tarpusavyje pirminiai su moduliu. Jeigu taip padarysime su mažiausių teigiamų liekanų sistema

$$1, 2, \ldots, m,$$

tai liks skaičiai, ne didesni už m ir tarpusavyje pirminiai su m.

Jau minėjome, kad Oilerio funkcijos reikšmė $\varphi(m)$ reiškia skaičių natūrinių skaičių, ne didesnių už m ir tarpusavyje pirminių su m. Todėl teisingas toks teiginys apie r. l. s. elementų skaičių: *redukuotoji liekanų sistema moduliu m turi $\varphi(m)$ elementų.*

Suformuluosime redukuotosios liekanų sistemos sudarymo kriterijų.

Kad $\varphi(m)$ skaičių sudarytų redukuotąją liekanų sistemą moduliu m, būtina ir pakankama, kad jie būtų tarpusavyje pirminiai su moduliu m ir jokie du iš jų nelygtų vienas kitam tuo moduliu.

Iš tikrųjų, jei nėra tarp tų skaičių lygstančių vienas kitam moduliu m, tai visi jie atstovauja skirtingoms liekanų klasėms, tarpusavyje pirminėms su moduliu; tų skaičių yra tiek, kiek yra tokių klasių.

Pavyzdžiai. 1. Sudarysime r. l. s. moduliu 5. Iš penkių liekanų klasių moduliu 5:

$$K_0, K_1, K_2, K_3, K_4$$

tik pirmoji nėra tarpusavyje pirminė su moduliu, taigi $\varphi(5)=4$. Iš kitų klasių bet kaip parinkę po atstovą, turėsime r. l. s. moduliu 5:

$$1, 2, -2, -1.$$

2. Moduliu 4 yra 4 liekanų klasės:

$$K_0, K_1, K_2, K_3.$$

Akivaizdu, kad tik klasės K_1 ir K_3 yra tarpusavyje pirminės su 4. Todėl $\varphi(4)=2$. Paėmę po vieną atstovą iš tų dviejų klasių, turėsime r. l. s. moduliu 4:

$$1, \quad -1.$$

Įrodysime teoremą, analogišką 49 teoremai.

50 teorema. *Jeigu x įgyja visas redukuotosios liekanų sistemos moduliu m reikšmes, tai ir ax pavidalo skaičiai sudaro redukuotąją liekanų sistemą tuo pačiu moduliu, kai $(a, m)=1$.*

Įrodymas. Tarkime, kad x įgyja visas reikšmes iš šios r. l. s. moduliu m:

$$b_1, b_2, \ldots, b_{\varphi(m)}. \tag{3.4}$$

Tuomet visos ax reikšmės sudaro skaičių seką

$$ab_1, ab_2, \ldots, ab_{\varphi(m)}. \tag{3.5}$$

Tų skaičių yra $\varphi(m)$, jokie du iš jų nelygsta moduliu m. Jeigu kuriuos nors du skaičius sietų lyginys

$$ab_i \equiv ab_j \pmod{m},$$

tai, remdamiesi teoremos sąlyga $(a, m)=1$, galėtume tą lyginį suprastinti:

$$b_i \equiv b_j \pmod{m}.$$

Gautasis lyginys prieštarautų prielaidai, kad (3.4) sekos skaičiai sudaro r. l. s. moduliu m. Taigi jokie du iš (3.5) sekos skaičių nelygsta vienas kitam moduliu m.

Taip pat nesunku įsitikinti, kad visi (3.5) sekos skaičiai yra tarpusavyje pirminiai su moduliu m. Iš tikrųjų, jeigu i – bet kuris numeris nuo 1 iki $\varphi(m)$, tai, remdamiesi 11 teorema ir tuo, kad skaičiai b_i yra tarpusavyje pirminiai su moduliu m, gauname

$$(ab_i, m)=(b_i, m)=1.$$

Pavyzdys. Skaičiai $-8, 2, 22, -4, 7, 17$ sudaro r. l. s. moduliu 9. Kadangi 2 ir 9 yra tarpusavyje pirminiai skaičiai, tai padauginę pateiktuosius skaičius iš 2, gausime r. l. s. moduliu 9:

$$-16, 4, 44, -8, 14, 34.$$

Uždaviniai

15. Įrodykite, kad skaičiai $41, -20, 24, 54, -21, 34, -9, 5$ sudaro p. l. s. moduliu 8.

16. Įrodykite, kad skaičiai $46, 40, -8, 48, 39, -12, -21, 27, 63, -35, -22$ sudaro p. l. s. moduliu 11.

17. Įrodykite, kad skaičiai $-11, 65, 95, 19$ sudaro r. l. s. moduliu 12.

18. Įrodykite, kad 5 iš eilės einantys sveikieji skaičiai sudaro p. l. s. moduliu 5.

19. Užrašykite absoliutiniu didumu mažiausias pilnąsias liekanų sistemas moduliais 20, 21, 22.

20. Remdamiesi 49 teorema, transformuokite mažiausių neneigiamų liekanų sistemą moduliu 9 imdami $a=-1, -2, k=1, 2$.

21. Įrodykite, kad iš r. l. s. moduliu 13, atlikę transformaciją $2x+1$, r. l. s. negauname.

22. Nustatykite, kiek galima sudaryti skirtingų p. l. s. ir r. l. s. moduliu 6 iš vienaženklių sveikųjų skaičių.

23. Užrašykite tris p. l. s. moduliu 6, sudarytas iš $-5x+2$ pavidalo skaičių.

24. Įrodykite teiginį: jeigu x įgyja reikšmes iš pilnosios liekanų sistemos moduliu m_1, y įgyja reikšmes iš pilnosios liekanų sistemos moduliu m_2 ir $(m_1, m_2)=1$, tai xm_2+ym_1 įgyja reikšmes iš pilnosios liekanų sistemos moduliu m_1m_2.

§30. Liekanų klasių, tarpusavyje pirminių su moduliu, grupė

27 paragrafe nustatėme, kad struktūra $L_m=(\mathbf{Z}/(m), +, \cdot)$ yra komutatyvusis žiedas su vienetu. Liekanų klasių moduliu m aibė su sudėtimi $(\mathbf{Z}/(m), +)$ yra *adicinė grupė*.

Liekanų klasių moduliu m aibėje apibrėžta daugyba, tačiau ta aibė nėra multiplikacinė grupė. Iš tikrųjų šios aibės nulinis elementas – liekanų klasė K_0 – neturi atvirkštinio elemento. Tokio elemento gali neturėti ir nenulinės klasės. Pavyzdžiui, 28 paragrafe sudarytoje liekanų klasių moduliu 6 daugybos lentelėje matome, kad klasės K_2, K_3, K_4 taip pat neturi atvirkštinių elementų: pavyzdžiui, su jokia liekanų klase K_x moduliu 6 nėra išpildoma sąlyga $K_2 \cdot K_x=K_1$.

Kitaip yra, kai nagrinėjama tik tarpusavyje pirminių su moduliu liekanų klasių tuo moduliu aibė. Ši aibė gali nesudaryti adicinės grupės. Iš tikrųjų, kai $m \geqslant 2$, liekanų klasių K_1 ir K_{m-1}, tarpusavyje pirminių su moduliu m,

suma – liekanų klasė K_m jau nėra tarpusavyje pirminė su moduliu. Tačiau ta aibė yra multiplikacinė grupė.

51 teorema. *Liekanų klasės moduliu m, tarpusavyje pirminės su moduliu, sudaro* $\varphi(m)$ *eilės multiplikacinę grupę.*

Įrodymas. Liekanų klasių moduliu m aibėje daugyba apibrėžta lygybe

$$K_a \cdot K_b = K_{ab}.$$

Liekanų klasių moduliu m, tarpusavyje pirminių su tuo moduliu, sandauga yra tarpusavyje pirminė su m, nes iš $(a, m)=(b, m)=1$ išplaukia

$$(K_{ab}, m)=(ab, m)=1.$$

Įrodysime, kad kiekviena liekanų klasė K_a moduliu m, kai $(a, m)=1$, turi atvirkštinį elementą.

Tarkime, kad x įgyja visas redukuotosios liekanų sistemos moduliu m reikšmes. Iš 50 teoremos išplaukia, kad ir sandauga ax įgyja visas redukuotosios liekanų sistemos reikšmes. Todėl egzistuoja tokia x reikšmė $x=c$, su kuria teisingas lyginys

$$ac \equiv 1 \pmod{m},$$

nes liekanų klasė K_1 priklauso su moduliu tarpusavyje pirminių klasių aibei, o tos klasės atstovu r. l. s. galima imti skaičių 1. Pastarasis lyginys ekvivalentus lygybei

$$K_a \cdot K_c = K_1.$$

Iš tikrųjų skaičiai ac ir 1 priklauso tai pačiai klasei moduliu m. Taigi K_c yra liekanų klasei K_a atvirkštinis elementas. Teorema įrodyta.

Jeigu modulis m yra pirminis skaičius p, tai tik viena – nulinė liekanų klasė K_0 nėra tarpusavyje pirminė su moduliu. Tarpusavyje pirminė su p yra $p-1$ klasė. Tiek elementų turi multiplikacinė liekanų klasių grupė G_p pirminiu moduliu p. Taigi adicinė liekanų klasių moduliu p grupė ir multiplikacinė liekanų klasių, tarpusavyje pirminių su moduliu p, grupė skiriasi tik vienu elementu – nuline liekanų klase. Išryškėja analogija su racionaliųjų skaičių aibe **Q**: visi racionalieji skaičiai sudaro adicinę grupę, o visi nelygūs nuliui racionalieji skaičiai – multiplikacinę grupę (aibėje **Q** apibrėžtų atitinkamų operacijų atžvilgiu).

Kaip žinome, racionaliųjų skaičių aibė **Q** sudėties ir daugybos operacijų atžvilgiu sudaro lauką. Analogiškas teiginys teisingas ir liekanų klasių pirminiu moduliu aibei.

52 teorema. *Liekanų klasių pirminiu moduliu p žiedas* L_p *yra laukas.*

Įrodymas. Komutatyvusis žiedas L_p yra laukas, nes jo kiekvienas nenulinis elementas $K_a \neq K_0$ turi atvirkštinį elementą – tai išplaukia iš 51 teoremos. Akivaizdu, kad su $m=p \geqslant 2$ išpildomos visos lauko apibrėžime nurodytos sąlygos.

Liekanų klasių pirminiu moduliu p laukas L_p yra baigtinis, nes aibė $\mathbf{Z}/(p)$ turi p elementų:

$$K_0,\ K_1,\ \ldots,\ K_{p-1}.$$

Kadangi pirminių skaičių yra be galo daug, tai tiek yra ir laukų L_p.

Pavyzdys. Rasime liekanų klasių moduliu 7 lauko elementui K_5 atvirkštinį elementą — tokį elementą K_x, su kuriuo būtų teisinga lygybė

$$K_5 \cdot K_x = K_1.$$

Daugindami K iš visų nenulinių liekanų klasių tuo moduliu, randame:

$$K_5 \cdot K_1 = K_5,\quad K_5 \cdot K_2 = K_3,\quad K_5 \cdot K_3 = K_1,$$

$$K_5 \cdot K_4 = K_6,\quad K_5 \cdot K_5 = K_4,\quad K_5 \cdot K_6 = K_2,$$

Taigi ne tik radome klasei K_5 atvirkštinį lauko elementą — klasę K_3, bet ir įsitikinome, kad toks elementas yra vienintelis.

Tą patį rezultatą galima gauti ir kitu keliu — ieškant tokio skaičiaus x, su kuriuo būtų teisingas lyginys

$$5x \equiv 1 \pmod 7.$$

Remsimės jau žinoma lyginių savybe — prie bet kurios lyginio pusės galima pridėti modulio kartotinį. Pridėsime prie lyginio dešiniosios pusės 14:

$$5x \equiv 15 \pmod 7.$$

Suprastinę abi lyginio puses iš 5 (kadangi 5 ir modulis — tarpusavyje pirminiai skaičiai, tai galime taikyti 47 teoremos išvadą), gauname

$$x \equiv 3 \pmod 7.$$

Taigi ieškomasis x priklauso liekanų klasei K_3.

Uždaviniai

25. Atlikite veiksmus su liekanų klasėmis moduliu 12:

$$K_2^2 + K_3^3,\quad K_4 \cdot K_5 \cdot K_6,\quad (K_3 + K_4)^2,\quad (K_3^2 + K_4^3)^2.$$

26. Raskite visų liekanų klasių moduliais 8, 9, 10, 11, tarpusavyje pirminių su moduliu, atvirkštines klases.

27. Liekanų klasių moduliu 13 aibėje išspręskite šias lygtis:

$$x^2 = K_1,\quad x^2 + x + K_2 = K_0,\quad K_2 K_7 x^2 = K_3 K_4.$$

§31. Oilerio funkcijos reikšmių skaičiavimas

Kaip minėjome, Oilerio funkcijos $\varphi(m)$ reikšmė lygi skaičiui natūrinių skaičių, ne didesnių už m ir tarpusavyje pirminių su m.

Įrodysime teoremą, kuria remdamiesi galėsime apskaičiuoti Oilerio funkcijos reikšmes, kai argumentas yra pirminis skaičius arba jo natūrinis laipsnis.

53 teorema. *Jeigu p^α yra pirminio skaičiaus natūrinis laipsnis, tai*

$$\varphi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right), \tag{3.6}$$

$$\varphi(p) = p - 1. \tag{3.7}$$

Įrodymas. Iš visų skaičių

$$1,\ 2,\ \ldots,\ p,\ p+1,\ \ldots,\ p^{\alpha}-1,\ p^{\alpha} \tag{3.8}$$

išbrauksime tuos, kurie turi bendrų daliklių su moduliu $m=p^{\alpha}$. Modulio dalikliai yra tik p laipsniai. Taigi (3.8) skaičių sekoje reikia išbraukti visus p kartotinius, nes tik jie turi bendrų daliklių su p^{α}. Pagal 1 teoremą tokių kartotinių yra

$$\left[\frac{p^{\alpha}}{p}\right]=p^{\alpha-1}.$$

Juos išbraukę, gauname

$$p^{\alpha}-p^{\alpha-1}=p^{\alpha}\left(1-\frac{1}{p}\right)$$

skaičių, ne didesnių už p^{α} ir tarpusavyje pirminių su p^{α}. (3.7) formulė gaunama iš (3.6) lygybės, kai $\alpha=1$.

Pavyzdžiui, rasime, kiek yra liekanų klasių, tarpusavyje pirminių su 81. Kadangi $81=3^4$, tai

$$\varphi(81)=3^4\left(1-\frac{1}{3}\right)=54.$$

Jeigu modulis m nėra pirminio skaičiaus natūrinis laipsnis, tai Oilerio funkcijos $\varphi(m)$ reikšmės apskaičiuojamos sudėtingiau. Norint gauti atitinkamą formulę, reikia detaliau išnagrinėti pačią funkciją.

54 teorema. *Oilerio funkcija yra multiplikatyvi, t. y. jeigu a ir b tarpusavyje pirminiai skaičiai, tai*

$$\varphi(ab)=\varphi(a)\,\varphi(b).$$

Įrodymas. Remsimės antruoju Oilerio funkcijos apibrėžimu. Tarkime, kad $(a,\ b)=1$. Apskaičiuosime $\varphi(ab)$. Skaičių sekoje

$$1,\ 2,\ \ldots,\ ab-1,\ ab$$

rasime, kiek yra skaičių, tarpusavyje pirminių su ab. Tos sekos skaičius surašome į lentelę, turinčią b eilučių ir a stulpelių:

$$\begin{array}{ccccc}
1, & 2, & 3, & \ldots, & a, \\
a+1, & a+2, & a+3, & \ldots, & 2a, \\
2a+1, & 2a+2, & 2a+3, & \ldots, & 3a, \\
\ldots\ldots\ldots & \ldots\ldots\ldots & \ldots\ldots\ldots & \ldots, & \ldots \\
(b-1)a+1, & (b-1)a+2, & b-1)a+3, & \ldots, & ba.
\end{array}$$

Visi k-ojo stulpelio skaičiai yra šitokie:

$$ca+k,\quad 0\leqslant c\leqslant b-1,$$

taigi visi jie priklauso tai pačiai liekanų klasei moduliu a. Kiekvienas stulpelis priklauso vis kitai liekanų klasei moduliu a, nes k kinta nuo 1 iki a. Išbraukiame stulpelius, priklausančius liekanų klasėms moduliu a, kurios

nėra tarpusavyje pirminės su a. Lieka $\varphi(a)$ stulpelių, kuriuose visi skaičiai jau tarpusavyje pirminiai su a.

Kiekviename stulpelyje yra b skaičių, kurie pagal 49 teoremą sudaro p. l. s. moduliu b. Iš tikrųjų k-ojo stulpelio skaičiai gauti iš skaičių

$$0,\ 1,\ 2,\ \ldots,\ b-1,$$

padauginus juos iš a ir prie sandaugų pridėjus pastovų dėmenį k. Kadangi $(a,\ b)=1$, tai 49 teoremos sąlygos yra išpildytos.

Išbraukę kiekviename stulpelyje, sudarančiame p. l. s. moduliu b, tuos skaičius, kurie nėra tarpusavyje pirminiai su b, matome, kad kiekviename iš likusių $\varphi(a)$ stulpelių yra $\varphi(b)$ skaičių, tarpusavyje pirminių ir su a, ir su b. Taigi lentelėje likę natūriniai skaičiai yra ne didesni už ab ir pirminiai su ab. Vadinasi,

$$\varphi(ab)=\varphi(a)\varphi(b).$$

Išvada. Jeigu $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, tai

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right).$$

Remdamiesi 54 ir 53 teoremomis, gauname

$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k})=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k}).$$

Rasime, pavyzdžiui, $\varphi(100)$. Kadangi $100=2^2\cdot 5^2$, tai

$$\varphi(100)=100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=40.$$

Iš Oilerio funkcijos apibrėžimo išplaukia, kad

$$\varphi(1)=1.$$

Oilerio funkcija — viena iš įdomiausių skaičių teorijos funkcijų. Pavyzdžiui, vokiečių matematikas K. Gausas išvedė formulę

$$\sum_{d\mid n}\varphi(d)=n. \tag{3.9}$$

Oilerio funkcijos reikšmės natūrinių skaičių aibėje išsibarsčiusios be regimos tvarkos. Pavyzdžiui,

$$\varphi(1)=1,\qquad \varphi(6)=2,$$
$$\varphi(2)=1,\qquad \varphi(7)=6,$$
$$\varphi(3)=2,\qquad \varphi(8)=4,$$
$$\varphi(4)=2,\qquad \varphi(9)=6,$$
$$\varphi(5)=4,\qquad \varphi(10)=4.$$

Nematome jokio $\varphi(n)$ reikšmių kitimo dėsningumo. Tačiau Oilerio funkcijos reikšmių vidurkiai didėja jau apibrėžta tvarka. Galima įrodyti, kad

$$\sum_{n=1}^{N} \varphi(n) = \frac{3}{\pi^2} N^2 + CN \ln N; \tag{3.10}$$

čia C – tam tikra konstanta. Iš tos lygybės išplaukia, kad Oilerio funkcijos reikšmių vidurkis intervale $[1, N]$ asimptotiškai lygus

$$\frac{3}{\pi^2} N.$$

Uždaviniai

28. Nustatykite, kada $\varphi(2x) = 2\varphi(x)$.

29. Išspręskite lygtis $\varphi(x) = 2^\alpha$, $\varphi(5^x) = 100$, $\varphi(x) = 8$, $\varphi(x) = 12$.

30. Nustatykite, kuris iš skaičių $\varphi(mn)$ ir $\varphi(m)\varphi(n)$ yra didesnis, kai $(m, n) > 1$.

31. Įrodykite, kad $\varphi(ab) = \varphi(a, b)\varphi([a, b])$.

32. Kiek yra mažesnių už 50 dviženklių natūrinių skaičių, kurie nėra tarpusavyje pirminiai su 50?

33. Įrodykite lygybes $\varphi(4x+2) = \varphi(2x+1)$, $\varphi(4x) = 2\varphi(x)$, kai x – nelyginis.

34. Apskaičiuokite Oilerio funkcijos reikšmes $\varphi(24)$, $\varphi(40)$, $\varphi(120)$, $\varphi(1000)$, $\varphi(1250)$, $\varphi(6^6)$, $\varphi(2^2 \cdot 3^3 \cdot 4^2 \cdot 5^3)$.

§32. Oilerio ir Ferma teoremos

Vienas iš gražiausių klasikinės skaičių teorijos rezultatų yra toliau pateikiama teorema.

Oilerio teorema. *Jeigu* $(a, m) = 1$, *tai*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Įrodymas. Tarkime, kad skaičiai $b_1, b_2, \ldots, b_{\varphi(m)}$ sudaro r. l. s. moduliu m. Kadangi $(a, m) = 1$, tai iš 50 teoremos išplaukia, jog skaičiai

$$ab_1, ab_2, \ldots, ab_{\varphi(m)}$$

taip pat sudaro r. l. s. tuo moduliu. Todėl teisingi lyginiai

$$\begin{aligned} ab_1 &\equiv b_{s_1} \pmod{m}, \\ ab_2 &\equiv b_{s_2} \pmod{m}, \\ &\cdots\cdots\cdots\cdots \\ ab_{\varphi(m)} &\equiv b_{s_{\varphi(m)}} \pmod{m}. \end{aligned}$$

Lyginių dešiniosiose pusėse esantys skaičiai sudaro aibę $b_1, b_2, \ldots, b_{\varphi(m)}$, tik galbūt jie išsidėstę kitaip, negu kairiosiose lyginių pusėse esantys b_i, t. y.

$$\{s_1, s_2, \ldots, s_{\varphi(m)}\} = \{1, 2, \ldots, m\}.$$

Taigi

$$b_1 b_2 \ldots b_{\varphi(m)} \equiv b_{s_1} b_{s_2} \ldots b_{s_{\varphi(m)}} \pmod{m}.$$

Sudauginę panariui visus $\varphi(m)$ lyginių ir pasinaudoję pastarąja lygybe, gauname

$$a^{\varphi(m)} b_1 b_2 \ldots b_{\varphi(m)} \equiv b_1 b_2 \ldots b_{\varphi(m)} \pmod{m}.$$

Kadangi skaičiai b_i tarpusavyje pirminiai su moduliu m (nes jie sudaro r. l. s), tai galime iš jų suprastinti abi pastarojo lyginio puses. Gausime teoremoje nurodytą lyginį.

Oilerio teoremą galime įrodyti ir trumpesniu būdu, remdamiesi grupių teorija. 51 teoremoje įrodėme, kad liekanų klasės, tarpusavyje pirminės su moduliu m, sudaro $\varphi(m)$ eilės multiplikacinę grupę. Vadovėlio I dalyje Lagranžo teoremos išvadoje tvirtinama, kad grupės eilė dalijasi iš bet kurio jos elemento eilės. Vadinasi, jeigu $(a, m)=1$ ir liekanų klasės K_a eilė yra δ, tai

$$K_a^{\delta} = K_1.$$

Pakėlę abi šios lygybės puses natūriniu laipsniu $\varphi(m)/\delta$, gauname

$$K_a^{\varphi(m)} = K_1.$$

Pastaroji lygybė ekvivalenti lyginiui

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Atskiras Oilerio teoremos atvejis vadinamas *Ferma* vardu.

Ferma teorema. *Jeigu p yra pirminis skaičius, a — sveikasis skaičius ir $(a, p)=1$, tai*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Įrodymas išplaukia iš Oilerio teoremos, paėmus $m=p$.

55 teorema. *Jeigu p yra pirminis skaičius, tai su visais sveikaisiais a*

$$a^p \equiv a \pmod{p}. \tag{3.11}$$

Įrodymas. Jeigu $(a, p)=1$, tai teiginys išplaukia iš Ferma teoremos. Jeigu $(a, p)=p$, tai abi (3.11) lyginio pusės dalijasi iš p ir todėl $p \mid a^p - a$.

Remdamiesi Oilerio ir Ferma teoremomis, galime rasti liekanas, kurias gauname dalydami sveikųjų skaičių natūrinius laipsnius iš m.

Pavyzdžiai. 1. Rasime liekaną, kurią gautume dalydami 5^{121} iš 7. Pagal Ferma teoremą

$$5^6 \equiv 1 \pmod{7}.$$

Keliame abi lyginio puses 20 laipsniu:

$$5^{120} \equiv 1 \pmod{7}.$$

Padauginę abi lyginio puses iš 5, gauname

$$5^{121} \equiv 5 \pmod{7}.$$

Ieškomoji liekana lygi 5.

2. Rasime liekaną, kurią gautume dalydami sumą $5^{100}+9^{100}$ iš 14. Pagal Oilerio teoremą

$$5^{\varphi(14)} = 5^6 \equiv 1 \pmod{14}, \quad 9^6 \equiv 1 \pmod{14}.$$

Toliau gauname

$$5^{96} \equiv 1 \pmod{14}, \qquad 9^{96} \equiv 1 \pmod{14},$$

$$5^{100} \equiv 9 \pmod{14}, \qquad 9^{100} \equiv 9 \pmod{14}.$$

Taigi

$$5^{100} + 9^{120} \equiv 18 \equiv 4 \pmod{14}.$$

Liekana lygi 4.

Uždaviniai

35. Raskite p, kai $5^{p^2} + 1 \equiv 0 \pmod{p}$.

36. Raskite

$$\sum_{d \mid m} \varphi\left(\frac{m}{d}\right).$$

37. Raskite liekanas, kurias gautume dalydami šiuos skaičius: 3^{1000} iš 17, 12^{100} iš 29, $4^{50} - 30^{50}$ iš 11, $5^{100} + 5^{200} + 5^{300}$ iš 11, a^{100} iš 125.

38. Įrodykite: jeigu $(a, p) = 1$, p – pirminis skaičius, tai

$$a^{kp+1-k} \equiv a \pmod{p}.$$

§33. Lyginių taikymai

Dalumo požymiai. Naudodamiesi lyginiais, išvesime kai kuriuos dalumo požymius.

Tarkime, kad natūrinis skaičius N užrašytas skaičiavimo sistemoje pagrindu g:

$$N = b_0 + b_1 g + b_2 g^2 + \ldots + b_r g^r.$$

Jeigu skaičių N, užrašytą sistemoje pagrindu g, suskirstysime iš dešinės į kairę grupėmis po k skaitmenų b_i (kairioji grupė gali turėti ir mažiau skaitmenų), tai gautieji k-ženkliai skaičiai $n_0, n_1, \ldots, n_s$ (sistemoje pagrindu g) yra skaičiaus N skaitmenys sistemoje pagrindu g^k (plg. § 9). Sakykime,

$$n = \overline{a_{k-1} a_{k-2} \ldots a_1 a_0}_{(g)}$$

yra k-ženklis skaičius. Tada $n \geqslant 0$ ir, be to,

$$n = a_{k-1} g^{k-1} + a_{k-2} g^{k-2} + \ldots + a_1 g + a_0 \leqslant (g-1) g^{k-1} +$$

$$+ (g-1) g^{k-2} + \ldots + (g-1) g + g - 1 = (g-1)(g^{k-1} +$$

$$+ g^{k-2} + \ldots + g + 1) = (g-1) \frac{g^{k-1}}{g-1} < g^k.$$

Pavyzdys. Jeigu $g = 10$, N = 3 100 127 016, $k = 3$, tai suskirstymas

$$N = 3 \mid 100 \mid 127 \mid 016$$

tolygus skaičiaus N užrašymui sistemoje pagrindu 10^3 su skaitmenimis

$$n_3 = 3, \quad n_2 = 100, \quad n_1 = 127, \quad n_0 = 16,$$

arba

$$N = 3 (10^3)^3 + 100 (10^3)^2 + 127 (10^3) + 16.$$

Pagal skaičių n, n_1, ..., n_s apibrėžimą

$$N = \sum_{i=0}^{r} b_i g^i = \sum_{j=0}^{s} n_j (g^k)^j. \tag{3.12}$$

Tarkime, kad skaičius k apibrėžtas lyginiu

$$g^k \equiv 1 \pmod{m}. \tag{3.13}$$

Tuomet iš (3.12) lygybės išplaukia

$$N = \sum_{j=0}^{s} n_j \pmod{m}.$$

Analogiškai, jeigu skaičių k apibrėžiame lyginiu

$$g^k \equiv -1 \pmod{m}, \tag{3.14}$$

tai iš (3.12) lygybės išplaukia lyginys

$$N \equiv \sum_{j=0}^{s} (-1)^j n_j \pmod{m}.$$

Remiantis gautaisiais rezultatais galima suformuluoti dalumo požymių nustatymo taisyklę.

Skaičių N, užrašytą skaičiavimo sistemoje pagrindu g, iš dešinės į kairę suskirstome grupėmis po k skaitmenų (kairioji grupė gali likti nepilna) ir tas grupes laikome k-ženkliais skaičiais. Skaičius N dalijasi iš skaičiaus m, tarpusavyje pirminio su g, tada ir tik tada,, kai iš m dalijasi gautųjų k-ženklių skaičių algebrinė suma. Pastarojoje sumoje visi dėmenys imami teigiami, jei k apibrėžtas (3.13) *sąlyga, ir jų ženklai keičiami pakaitomis, jei k apibrėžtas* (3.14) *sąlyga.*

Pavyzdžiai. 1. Dešimtainėje sistemoje išvesime dalumo iš 11 požymį. Kadangi $10^2 \equiv 1 \pmod{11}$, tai pagal anksčiau suformuluotą taisyklę *skaičius N dalijasi iš* 11 *tada ir tik tada, kai iš* 11 *dalijasi suma dviženklių skaičių, į kuriuos N suskirstomas iš dešinės.*

Skaičius $N = 83\,010\,002\,042$ dalijasi iš 11, nes, suskirstę jį grupėmis po 2 skaitmenis:

$$N = 8 \mid 30 \mid 10 \mid 00 \mid 20 \mid 42$$

ir sudėję gautuosius dviženklius skaičius, gauname iš 11 besidalijantį skaičių:

$$8 + 30 + 10 + 20 + 42 = 110.$$

2. Išvesime kitą skaičių dalumo iš 11 požymį dešimtainėje sistemoje. Kadangi

$$10^1 \equiv -1 \pmod{11},$$

tai, norint nustatyti dalumo požymį, skaičių N reikia suskirstyti į grupes po 1 skaitmenį. Tačiau tokios grupės — tai tie patys skaičiaus N skaitmenys. Taigi gauname dar vieną dalumo iš 11 kriterijų: *skaičius N dalijasi iš* 11 *tada ir tik tada, kai iš* 11 *dalijasi jo skaitmenų su pakaitomis besikeičiančiais ženklais suma.*

Pavyzdžiui, skaičius $N = 411\,071$ iš 11 nesidalija, nes iš 11 nesidalija skaitmenų su besikeičiančiais ženklais suma:

$$4 - 1 + 1 - 0 + 7 - 1 = 10.$$

3. Kadangi

$$10^1 \equiv 1 \pmod 9,$$

$$10^1 \equiv 1 \pmod 3,$$

tai gauname mums jau žinomus dalumo iš 9 ir 3 požymius: *skaičius dalijasi iš* 9 *arba* 3, *kai iš* 9 *arba* 3 *dalijasi jo skaitmenų suma.*

4. Išvesime dalumo iš 7 požymį aštuonetainėje sistemoje. Kadangi

$$8^1 \equiv 1 \pmod 7,$$

tai skaičius dalijasi iš 7, kai aštuonetainėje sistemoje iš 7 dalijasi jo skaitmenų suma. Pavyzdžiui, aštuonetainės sistemos skaičius

$$40003_8$$

dalijasi iš 7.

Išnagrinėsime dar vieną dalumo požymį, kuris žinomas *Paskalio teoremos* pavadinimu.

56 (Paskalio) teorema. *Tarkime, kad skaičius N užrašytas sistemoje pagrindu g:*

$$N = a_s g^s + a_{s-1} g^{s-1} + \ldots + a_1 g + a_0$$

ir

$$g^k \equiv b_k \pmod m \quad (\forall k,\ 1 \leqslant k \leqslant s).$$

Skaičius N dalijasi iš m tada ir tik tada, kai iš m dalijasi suma

$$\sum_{k=0}^{s} a_k b_k.$$

Įrodymas. Lygybę, kuria apibrėžtas N, reikia pakeisti lyginiu moduliu m.

Pavyzdys. Skaičius N užrašytas dvejetainėje sistemoje:

$$N = 1001001_2.$$

Aiškinsimės, ar tas skaičius dalijasi iš 7. Kadangi

$$N = 2^6 + 2^3 + 1,$$

$$2^3 \equiv 1 \pmod 7, \quad 2^6 \equiv 1 \pmod 7,$$

tai

$$\sum a_k b_k = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 = 3.$$

Vadinasi, skaičius N iš 7 nesidalija.

Įrodysime dar vieną dalumo požymį.

57 teorema. *Dešimtainės sistemos skaičius N dalijasi iš* 2^n (5^n), *kai iš* 2^n (5^n) *dalijasi n-ženklis skaičius, sudarytas iš n paskutinių skaičiaus N skaitmenų.*

Įrodymas. Atskyrę skaičiaus

$$N = \overline{a_s \ldots a_n a_{n-1} \ldots a_0}_{(10)}$$

paskutinius n skaitmenų, turime:

$$N = \overline{a_s \ldots a_n}_{(10)} \cdot 10^n + \overline{a_{n-1} \ldots a_0}_{(10)}.$$

Dabar teoremos tvirtinimas akivaizdus.

Pavyzdžiui, skaičius 75 001 860 012 iš 16 nesidalija, nes iš $16 = 2^4$ nesidalija skaičius, sudarytas iš paskutinių 4 to skaičiaus skaitmenų, t. y. skaičius 12.

Aritmetinių veiksmų tikrinimas. Lyginių teorija taikoma ir aritmetinių veiksmų rezultatams tikrinti.

Pavyzdžiui, sudauginę 3 skaičius A, B ir C, gavome skaičių D. Norime patikrinti tą rezultatą nebekartodami daugybos. Jeigu

$$D = ABC,$$

tai

$$D \equiv ABC \pmod{m};$$

čia m – bet koks skaičius. Jeigu

$$A \equiv a \pmod{m}, \quad C \equiv c \pmod{m},$$

$$B \equiv b \pmod{m}, \quad D \equiv d \pmod{m},$$

tai

$$d \equiv abc \pmod{m}.$$

Reikia pasirinkti tokius modulius, kuriais lengva rasti liekanas, tuomet lengviau tikrinti. Patogu moduliais imti 9 ir 11, nes jų dalumo požymiai paprasti.

Tačiau, jeigu atlikdami veiksmus padarėme tokią klaidą, kad tikrasis rezultatas nuo gautojo skiriasi skaičiaus m sveikuoju kartotiniu:

$$D' = D + mt,$$

tai tikrindami moduliu m tos klaidos nerasime, nes

$$D' \equiv D \pmod{m}.$$

Naudojantis dviem moduliais, tikimybė, kad liks nepastebėta klaida, žymiai sumažėja.

Pavyzdžiai. 1. $c = 47131 \cdot 35809 = 1687713979$.
Iš pradžių tikrinsime moduliu 9.

$$a = 47131 \equiv 4+7+1+3+1 \equiv 7 \pmod 9,$$

$$b = 35809 \equiv 3+5+8+9 \equiv 7 \pmod 9,$$

$$ab \equiv 49 \equiv 4 \pmod 9,$$

$$c \equiv 1+6+8+7+7+1+3+9+7+9 \equiv 13 \equiv 4 \pmod 9.$$

Kadangi $ab \equiv c \pmod 9$, tai arba sudauginta teisingai, arba teisingas rezultatas skiriasi nuo pateiktojo skaičiumi, lygiu 9 kartotiniui.

Patikrinsime dar ir moduliu 11. Dalumo kriterijus – reikia rasti skaitmenų algebrinę sumą su pakaitomis besikeičiančiais ženklais. Visiems skaičiams ženklus reikia taip keisti, kad paskutiniai skaitmenys būtų vienodų ženklų. Ženklų keitimo tvarka nesvarbi – pir-

majam skaitmeniui galima priskirti bet kokį ženklą, o kitų ženklus reikia nuosekliai keisti. Tikrinant veiksmus, skaičiai gali turėti nevienodai skaitmenų. Tuomet ženklus reikia taip surašyti, kad visuose skaičiuose vienodi skyriai turėtų tą patį ženklą. Todėl galima taip surašyti ženklus, kad, pavyzdžiui, paskutiniai skaitmenys būtų teigiami.

Taigi

$$a=47131\equiv 4-7+1-3+1\equiv -4 \pmod{11},$$

$$b=35809\equiv 3-5+8-0+9\equiv 4 \pmod{11},$$

$$ab\equiv -16\equiv 6 \pmod{11},$$

$$c\equiv -1+6-6+7-7+1-3+9-7+9\equiv 6 \pmod{11},$$

$$c\equiv ab \pmod{11}.$$

Vadinasi, arba ta sandauga teisinga, arba tikrasis rezultatas skiriasi nuo gautojo modulių 9 ir 11 sandaugos kartotiniu.

2. Patikrinsime rezultatą

$$\frac{5839131309}{57377}=95417.$$

Santykį perrašome sveikųjų skaičių lygybe

$$57377\cdot 95417=5839131309.$$

Tikriname moduliu 11:

$$a=57377\equiv 5-7+3-7+7\equiv 1 \pmod{11},$$

$$b=95417\equiv 9-5+4-1+7\equiv 3 \pmod{11}.$$

$$ab\equiv 3 \pmod{11}.$$

$$c=5839131309\equiv -5+8-3+9-1+3-1+3-0+9\equiv 6 \pmod{11}.$$

Kadangi $ab\not\equiv c \pmod{11}$, tai rezultatas neteisingas.

Lyginių taikymas Diofanto lygtims spręsti. Lyginius galima taikyti tiriant, ar egzistuoja kai kurių neapibrėžtųjų lygčių (Diofanto lygčių) sprendiniai. Išnagrinėsime keletą pavyzdžių.

1. Išsiaiškinsime, ar lygtis

$$17x^5+3x-14=0$$

išsprendžiama sveikaisiais skaičiais.

Imkime $m=5$. Pagal 55 teoremą lyginys

$$x^5\equiv x \pmod{5}$$

teisingas su visais sveikaisiais x. Todėl su visais tokiais x

$$17x^5+3x\equiv 17x+3x\equiv 20x\equiv 0 \pmod{5}.$$

Tačiau $14\not\equiv 0 \pmod{5}$. Taigi lygtis neturi sveikųjų sprendinių.

2. Įrodysime, kad Diofanto lygtis

$$x^2-2y^2+8z=3$$

neišsprendžiama.

Jeigu ši lygtis būtų išsprendžiama, tai būtų teisingas teiginys

$$x^2-2y^2+8z\equiv 3 \pmod{2},$$

arba

$$x^2 \equiv 1 \pmod 2.$$

Taigi x turi būti nelyginis skaičius. Pažymime

$$x = 2t + 1$$

ir įrašome į lygtį:

$$4t(t+1) - 2y^2 + 8z = 2,$$

arba

$$2t(t+1) - y^2 + 4z = 1.$$

Sulyginame abi lygties puses moduliu 4.

Kadangi dviejų greta esančių sveikųjų skaičių t ir $t+1$ sandauga yra lyginis skaičius, tai iš pastarosios lygybės išplaukia

$$-y^2 \equiv 1 \pmod 4.$$

Nesunku įsitikinti, kad bet kurio sveikojo skaičiaus a kvadratas

$$a^2 \not\equiv -1 \pmod 4.$$

Tai ir įrodo, kad Diofanto lygtis neturi sprendinių.

Kiti lyginių taikymai. Nagrinėjome porą lyginių taikymų matematikoje. Lyginius galime taikyti ir kai kuriems ekonomikos, technikos bei kitų mokslų uždaviniams. Pateiksime dar porą lyginių taikymo pavyzdžių.

1. Žingsniai ratu. Štampavimo automate ant nejudančios ašies sukasi ratas, ant jo lanko vienodais atstumais pritvirtinta N detalių. Štampavimo automato presui apdorojus vieną detalę, ratas pasisuka per h detalių.

Koks turi būti h, kad būtų suštampuotos visos detalės?

Tarkime, kad detalių numeriai sudaro kokią nors pilnąją liekanų sistemą moduliu N. Sakykime, štampavimo presas yra ties detale, kurios numeris n. Po vieno štampavimo žingsnio ratas pasisuko per h detalių, ir presas yra ties detale, kurios numeris $n+h$. Po 2 žingsnių priešais štampavimo presą atsisuks detalė, kurios numeris $n+2h$ ir t. t. Tarkim, kad po s žingsnių priešais štampavimo presą bus ta pati pirmoji detalė su numeriu n. Kadangi įvyko s pasisukimų, tai tos pačios detalės numeris (jei leistume numeriams nurodyta tvarka didėti) yra $n+sh$. Sudarome lyginį

$$n + sh \equiv n \pmod N.$$

Jeigu $(h, N) = 1$, tai iš šio lyginio išplaukia

$$s \equiv 0 \pmod N.$$

Mažiausia natūrinė s reikšmė, tenkinanti šią sąlygą, yra $s = N$. Sujungę briežinyje tuos apskritimo taškus, kurie atitinka detalių vietas rate, gauname taisyklingąjį N-kampį.

Vadinasi, jeigu pradėsime štampuoti nuo bet kurios detalės ir toliau štampuosime kas h-ąją detalę, kai $(h, N) = 1$, tai po N žingsnių suštampuosime visas N detalių (nė viena nebus du kartus štampuota).

Pažymėsime, kad šis pavyzdys – tai vienas iš prancūzų matematiko *Puanso* (1777–1859) pateiktų teiginių. Puanso mėgino kurti skaičių teoriją remdamasis vien skaičiaus ir tvarkos sąvokomis.

Paliksime skaitytojui įrodyti šitokį Puanso teiginį: jeigu n yra toks mažiausias natūrinis skaičius, kad nb dalijasi iš a, tai

$$(a, b) = a/n.$$

2. Savaitės dienų nustatymas. Tarkime, kad reikia nustatyti, kuri savaitės diena buvo 1918 metų vasario 16.

Išvesime formulę savaitės dienoms apskaičiuoti. Dabartinis kalendorius buvo įvestas 1582 metais, todėl apsiribosime taisykle, tinkančia tik vėlesniems metams.

Kaip žinome, keliamieji yra kas ketvirti metai – jų paskutiniai du skaitmenys sudaro iš 4 dalų dviženklį skaičių. Jeigu metai užrašomi dviem nuliais besibaigiančiu skaičiumi, tai keliamieji yra tik tie metai, kurių pirmieji du skaitmenys sudaro iš 4 dalų dviženklį skaičių (pavyzdžiui, 1600, 2000).

Keliamųjų metų papildoma diena – vasario 29 – pastumia kovo 1-ąją viena diena toliau. Pakanka nustatyti tiriamųjų metų kovo 1-osios savaitės dieną. Sudarant formulę, patogiau kovo mėnesį laikyti pirmuoju mėnesiu, balandį – antruoju ir t. t., vasarį – dvyliktuoju. Taip nustatytą mėnesio numerį žymėsime m.

Pradedame skaičiuoti nuo 1600 metų kovo 1 d. Ta diena buvo trečiadienis. Po 1600 metų ėjusius metus galima užrašyti šitaip:

$$N = c \cdot 100 + Y;$$

čia c – šimtmečių skaičius, Y – šimtmečio metų numeris. Atsižvelgę į anksčiau nurodytas keliamųjų metų skaičiavimo taisykles, po nesudėtingų skaičiavimų randame N-ųjų metų kovo 1 d. savaitės dienos numerio s išraišką:

$$s \equiv 3 - 2c + Y + \left[\frac{c}{4}\right] + \left[\frac{Y}{4}\right] \pmod 7. \qquad (3.15)$$

Ši formulė gaunama prie skaičiaus

$$3 + (100c + Y - 1600)$$

pridėjus įprastą keliamųjų metų pataisą

$$\frac{1}{4}(100c + Y - 1600)$$

ir atėmus šimtmečių pataisą

$$\frac{1}{4}(c - 16).$$

Laužtiniai skliaustai čia visur reiškia skaičiaus sveikąją dalį.

Iš (3.15) formulės randame, kad 1918 metų kovo 1 diena ($c = 19$, $Y = 18$) buvo penktadienis, nes

$$s \equiv 3 - 38 + 18 + 4 + 4 \equiv -2 \equiv 5 \pmod 7.$$

Dabar jau nesunku nustatyti, kad 1918 metų vasario 16 diena buvo šeštadienis.

Analogiškai galėtume išvesti formulę X metų M-ojo mėnesio d-osios dienos savaitės dienai s nustatyti. Formulė būtų šitokia:

$$s \equiv d + \frac{1}{5}(13M^* - 1) + Y^* + \left[\frac{1}{4}c\right] + \left[\frac{1}{4}Y^*\right] - 2c \pmod 7;$$

čia

$$c = \left[\frac{Y}{100}\right], \quad Y = X - 100c, \quad M \in \{1, 2, 3, \ldots, 12\},$$

$$Y^* = \begin{cases} Y, & M > 2, \\ Y - 1, & 1 \leqslant M \leqslant 2, \end{cases} \qquad M^* = \begin{cases} M - 2, & M > 2, \\ M + 10, & 1 \leqslant M < 2. \end{cases}$$

Pavyzdžiui, rasime, kuri savaitės diena buvo 1988 metų vasario 5-oji Šiuo atveju

$$c = 19, \quad Y = 88, \quad M = 2, \quad d = 5, \quad Y^* = 87, \quad M^* = 12.$$

Iš formulės randame

$$s \equiv 5 + 31 + 87 + 4 + 21 - 38 \equiv 5 \pmod 7.$$

Taigi 1988 metų vasario 5 buvo penktadienis.

Uždaviniai

39. Remdamiesi dalumo požymiais, nustatykite, ar skaičiai 977 132, 32 113 169, 386 073 689, 96 736 068 dalijasi iš 7, 11, 13.

40. Taikydami lyginius, patikrinkite, ar teisingai atlikti aritmetiniai veiksmai:

$$3745 \cdot 8067 = 30\,210\,915, \quad 8624 \cdot 5201 = 42\,981\,064,$$

$$423\,805\,807 : 43 = 9\,855\,949, \quad 3125 \cdot 9971 = 28\,323\,345,$$

$$31\,751 \cdot 4127 = 134\,172\,317, \quad 973\,126 : 979 = 974.$$

41. Įrodykite, kad Diofanto lygtys

$$x^2 + 47y^2 = 73, \quad 132x^2 + 63y^2 = 131$$

neišsprendžiamos.

42. Raskite, kuri savaitės diena bus:

1) 1991 metų sausio 31;
2) 1992 metų kovo 15;
3) 1999 metų gruodžio 31.

Lyginiai su kintamaisiais

§34. Lyginių su kintamaisiais sprendiniai

Nagrinėkime du lyginius: lyginį

$$3a+11\equiv 0 \pmod{13}, \tag{4.1}$$

a – sveikasis skaičius, ir lyginį

$$3\cdot 5+11\equiv 0 \pmod{13}. \tag{4.2}$$

Antrasis lyginys yra teisingas. Pirmasis lyginys gali būti ir teisingas, ir neteisingas, žiūrint koks yra skaičius a. Taigi (4.1) lyginys yra vienvietis predikatas, iš kurio, imdami konkrečią a reikšmę, galime gauti ir teisingą teiginį, ir neteisingą. Pavyzdžiui, kai $a=4$, (4.1) lyginys yra neteisingas.

Lyginiai, kuriuose, be skaičių, yra ir raidžių, yra *predikatai.* Galime nagrinėti, kada tokie lyginiai yra teisingi. Raides, įeinančias į lyginį, vadiname *kintamaisiais.*

Kaip įprasta matematikoje, kintamuosius žymėsime raidėmis x, y, z ir t. t. Atkreipsime skaitytojo dėmesį į tai, kad algebroje, sprendžiant lygtis su kintamaisiais, pastariesiems paprastai nekeliama jokių išankstinių sąlygų. Tačiau lyginiai apibrėžti tik sveikųjų skaičių žiede ir kintamieji lyginiuose gali įgyti tik sveikąsias reikšmes.

Šiame skyriuje nagrinėsime lyginius

$$f(x)\equiv 0 \pmod{m}; \tag{4.3}$$

čia $f(x)$ – polinomas su sveikaisiais koeficientais:

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1 x+a_0.$$

(4.3) pavidalo lyginius vadinsime *lyginiais su kintamuoju* x. Ieškosime tų sveikųjų x reikšmių, su kuriomis lyginys yra teisingas, kitaip sakant, *spręsime lyginį.*

(4.3) lyginio sprendimas žymiai skiriasi nuo analogiškos lygties

$$f(x)=0$$

sprendimo. Iš tikrųjų, kaip matėme praeitame skyriuje, (4.3) lyginys reiškia lygtį

$$f(x)=mt;$$

čia x ir t – kintamieji, galintys įgyti tik sveikąsias reikšmes. Taigi (4.3) lyginio sprendimas yra jam ekvivalenčios lygties su dviem kintamaisiais x ir t

sprendimas sveikųjų skaičių aibėje. Tai ženkliai sudėtingesnis uždavinys už lygties su vienu kintamuoju sprendimą.

Tarkime, kad radome tokią sveikąją x reikšmę a, su kuria lyginys yra teisingas. Imkime kokį nors sveikąjį skaičių b, kuris lygsta skaičiui a moduliu m:

$$b \equiv a \pmod{m}.$$

Pagal 27 paragrafe įrodytą 10-ąją lyginių savybę lyginys

$$f(b) \equiv f(a) \equiv 0 \pmod{m}$$

yra teisingas. Taigi jeigu (4.3) lyginys teisingas su kuriuo nors skaičiumi $x=a$, tai jis teisingas ir su bet kuriuo kitu skaičiumi $x=b$, kuris lygsta a moduliu m, t. y. su bet kuriuo skaičiumi iš liekanų klasės K_a moduliu m. Todėl sprendiniu laikysime ne kurį nors skaičių, o visą klasę K_a.

Lyginio su kintamuoju sprendiniu vadiname liekanų klasę, kurios skaičiai lyginį su kintamuoju paverčia teisingu teiginiu.

Aptarsime lyginių su kintamaisiais *ekvivalentumą*.

Lyginiai

$$f(x) \equiv 0 \pmod{m}$$

ir

$$F(x) \equiv 0 \pmod{M}$$

vadinami ekvivalenčiais, jei sutampa sveikųjų skaičių, tenkinančių tuos lyginius, aibės.

Jeigu $m=M$, tai lyginių ekvivalentumas reiškia, kad sutampa jų sprendiniai.

Pavyzdžiui, nesunku įsitikinti, kad lyginių

$$3x \equiv 1 \pmod{7} \quad \text{ir} \quad -6x \equiv 5 \pmod{7}$$

sprendiniai yra liekanų klasė K_5 moduliu 7. Vadinasi, tie lyginiai yra ekvivalentūs.

Jeigu $m \neq M$, tai lyginių sprendinių aibės nesutampa, nes jos yra liekanų klasės skirtingais moduliais. Tačiau sutampa atitinkamų skaičių, tenkinančių lyginius, aibės.

Pavyzdžiui, lyginiai

$$6x \equiv 2 \pmod{4} \quad \text{ir} \quad 3x \equiv 7 \pmod{2}$$

turi nevienodą skaičių sprendinių. Pirmojo lyginio sprendiniai yra du — tai liekanų klasės K_1 ir K_3 moduliu 4. Antrojo lyginio sprendinys yra vienas — liekanų klasė K_1 moduliu 2. Tačiau nesunku įsitikinti, kad ir pirmojo lyginio

du sprendiniai, ir antrojo lyginio vienas sprendinys apima tuos pačius – visus nelyginius – skaičius. Taigi šie lyginiai ekvivalentūs.

Lyginį be kintamojo galime laikyti lyginiu su kintamuoju, kuriame koeficientas prie kintamojo yra modulio kartotinis. Vadinasi, bet kurie du lyginiai be kintamojo yra ekvivalentūs.

Lyginio sprendinys žymimas įvairiai:

$$x = K_a,$$

$$x = a + mt, \quad t \in \mathbf{Z},$$

$$x \equiv a \pmod{m}.$$

Pavyzdžiui, (4.1) lyginio sprendinys yra liekanų klasė K_5 moduliu 13. Jį galime užrašyti ir šitaip: $x = 5 + 13t$, $t \in \mathbf{Z}$. Nuorodą $t \in \mathbf{Z}$ kartais praleisime. Mažosios lotyniškos raidės (jei kitaip nenurodyta) reiškia tik sveikuosius skaičius visur, kur kalbame apie lyginius.

Tarkime, kad nagrinėjame lyginį su kintamuoju x moduliu m. Šiuo moduliu yra m liekanų klasių. Todėl ir bet kuris lyginys su kintamuoju x moduliu m gali turėti ne daugiau kaip m sprendinių. Todėl galimas ir toks lyginio sprendimo būdas – patikrinti visas m liekanų klases ir nustatyti, kurios iš jų yra lyginio sprendiniai. Norint patikrinti, ar kokia nors liekanų klasė yra lyginio sprendinys, pakanka imti bet kurį skaičių a iš tos liekanų klasės ir nustatyti, ar lyginys su reikšme $x = a$ yra teisingas.

Pavyzdys. Išspręsime lyginį

$$3400x - 1713 \equiv 0 \pmod{7}.$$

Pirmiausia sumažiname lyginio koeficientus. Kadangi $3400 \equiv 5 \pmod{7}$, o $1713 \equiv 5 \pmod{7}$, tai lyginį su kintamuoju galime pakeisti jam ekvivalenčiu paprastesniu lyginiu

$$5x - 5 \equiv 0 \pmod{7}.$$

Remdamiesi 47 teoremos išvada, šio lyginio abi puses dalijame iš 5:

$$x - 1 \equiv 0 \pmod{7}.$$

Perkėlę -1 į dešiniąją pusę, gauname

$$x \equiv 1 \pmod{7}.$$

Tai labai paprastas lyginys, kurio, tiesą sakant, ir spręsti nebereikia. Gautasis lyginys ir yra atsakymas – sprendinys yra liekanų klasė K_1 moduliu 7. Visi x, su kuriais pradinis lyginys teisingas, yra $x = 1 + 7t$ pavidalo.

2. Išspręsime lyginį

$$49x^2 + 13x - 5 \equiv 0 \pmod{7}.$$

Prastindami, kaip ir pirmajame pavyzdyje, iš pastarojo lyginio gauname šitokį:

$$6x - 5 \equiv 0 \pmod{7}.$$

Moduliu 7 yra 7 liekanų klasės. Patikrinsime, kurios iš jų yra lyginio sprendiniai. Imsime po vieną atstovą iš visų 7 klasių – t. y. pilnąją liekanų sistemą moduliu 7. Galime imti mažiausių neneigiamų liekanų sistemą

$$0, 1, 2, 3, 4, 5, 6.$$

Lyginyje $6x - 5 \equiv 0 \pmod{7}$ paeiliui pakeitę kintamąjį x tais skaičiais, nustatome, kad tik su reikšme $x = 2$ gaunamas teisingas lyginys. Taigi pradinio lyginio sprendinys – liekanų klasė K_2 moduliu 7.

3. Spręsime lyginį

$$15135x \equiv 9751 \pmod{13}.$$

Kadangi

$$15135 \equiv 0 \pmod{13}, \quad 9751 \equiv 1 \pmod{13},$$

tai lyginys ekvivalentus šitokiam:

$$0 \cdot x \equiv 1 \pmod{13}.$$

Akivaizdu, kad šio lyginio netenkina joks sveikasis skaičius x. Taigi lyginys sprendinių neturi.

4. Išspręsime lyginį

$$15135x \equiv 9750 \pmod{13}.$$

Pertvarkę šį lyginį, gauname jam ekvivalentų lyginį

$$0 \cdot x \equiv 0 \pmod{m}.$$

Šis lyginys teisingas, kad ir koks būtų sveikasis skaičius x. Tai reiškia, kad sprendiniai yra visos 13 liekanų klasių:

$$K_0, K_1, K_2, \ldots, K_{12}.$$

Uždaviniai

1. Pakeiskite šiuos lyginius paprastesniais:

1) $4511x - 60001 \equiv 0 \pmod{2}$;
2) $10^{10}x + 10^9 \equiv 0 \pmod{7}$;
3) $343x^3 - 490x^2 + 1000x \equiv 10^{15} \pmod{7}$.

2. Išspręskite lyginius:

1) $-28x \equiv 4 \pmod{11}$;
2) $3x - 7 \equiv 18 \pmod{13}$;
3) $8x + 5 \equiv 3x - 1 \pmod{12}$;
4) $-200x \equiv -17 \pmod{11}$;
5) $17001x \equiv 45\ 000 \pmod{11}$;
6) $2^{45}x \equiv 3^{17} \pmod{7}$.

3. Nustatykite, su kuriomis a reikšmėmis neturi sprendinių šie lyginiai:

1) $51x + a \equiv 2 \pmod{11}$;
2) $(a+20)x \equiv 141 \pmod{13}$;
3) $379x + 80 \equiv a \pmod{17}$;
4) $41^{22}x + 17^{44} \equiv a + 2 \pmod{23}$;
5) $a^2 + 1 \equiv 0 \pmod{4}$;
6) $121a^3 - 55a^2 + 4\,(a+1)\,(a-1) \equiv 4a^5 + a \pmod{11}$.

§35. Pirmojo laipsnio lyginiai

Nagrinėsime pirmojo laipsnio lyginį

$$ax \equiv b \pmod{m}.$$

Nustatysime, su kokiomis a ir b reikšmėmis jis išsprendžiamas, pateiksime sprendimo būdų.

58 teorema. *Jeigu* $(a, m) = d$, *tai lyginys*

$$ax \equiv b \pmod{m} \qquad (4.4)$$

turi d sprendinių, kai d | b; jeigu K_{x_0} yra vienas iš to lyginio sprendinių, tai visi sprendiniai yra liekanų klasės, kurioms priklauso skaičiai

$$x_0,\ x_0+\frac{m}{d},\ x_0+2\,\frac{m}{d},\ \ldots,\ x_0+(d-1)\,\frac{m}{d}. \tag{4.5}$$

Jeigu $d\nmid b$, tai sprendinių nėra.

Įrodymas. Į (4.4) lyginį vietoj x įrašę bet kurį iš (4.5) skaičių, pavyzdžiui,

$$x_0+k\,\frac{m}{d}, \tag{4.6}$$

gauname

$$ax_0+\frac{a}{d}\,km\equiv b\ (\mathrm{mod}\ m),$$

arba

$$ax_0\equiv b\ (\mathrm{mod}\ m),$$

nes $d \mid a$ ir todėl santykis a/d yra sveikasis skaičius. Pastarasis lyginys teisingas, nes skaičius x_0 priklauso liekanų klasei, kuri yra (4.4) lyginio sprendinys. Vadinasi, ir (4.6) skaičius, t. y. bet kuris iš (4.5) skaičių priklauso atitinkamam sprendiniui.

Įsitikinsime, kad (4.5) skaičiai yra iš skirtingų liekanų klasių moduliu m. Iš tikrųjų, jeigu kurie nors du tos eilės skaičiai, pavyzdžiui,

$$x_0+k\,\frac{m}{d}\quad\text{ir}\quad x_0+j\,\frac{m}{d},\ \ 0\leqslant l\leqslant k\leqslant d-1,$$

lygtų moduliu m, tai iš lyginio

$$x_0+k\,\frac{m}{d}\equiv x_0+l\,\frac{m}{d}\ (\mathrm{mod}\ m)$$

išplauktų, kad

$$k\,\frac{m}{d}\equiv l\frac{m}{d}\ (\mathrm{mod}\ m),$$

arba

$$k\equiv l\,(\mathrm{mod}\ d),$$

nes $(m/d,\ m)=m/d$. Iš pastarojo lyginio išplaukia, kad $k-l$ dalijasi iš d, tačiau tik tada, kai $k=l$, nes $0\leqslant k-l<d$. Taigi (4.5) skaičiai priklauso d skirtingoms liekanų klasėms.

Lieka nustatyti, ar apskritai egzistuoja bent vienas sprendinys, t. y. ar galima rasti x_0, tenkinantį (4.4) lyginį.

(4.4) lyginį galima pakeisti lygtimi

$$ax=b+mt,$$

t. y. lygtimi

$$ax-mt=b$$

su dviem kintamaisiais x ir t. Tačiau 5 teoremos 2 išvada teigia, jog būtina ir pakankama sąlyga, kad ta lygtis būtų išsprendžiama, yra

$$d=(a,\ m)\mid b.$$

Išvada. *Jeigu* $(a,\ m)=1$, *tai lyginys*

$$ax\equiv b\ (\mathrm{mod}\ m)$$

visuomet turi vieną sprendinį.

Įrodysime teoremą apie liekanų klasių moduliu m suskaidymą į liekanų klases didesniais moduliais.

Pažymėsime, kad $K_a\subset K_b$, jei $b\mid a$.

59 teorema. *Liekanų klasė* K_a *moduliu* n *suskaidoma į* k *liekanų klasių moduliu* nk:

$$K_a,\ K_{a+n},\ K_{a+2n},\ \ldots,\ K_{a+(k-1)n}. \tag{4.7}$$

Įrodymas. Visų liekanų klasių skaičiai lygsta moduliu n, taigi priklauso vienai liekanų klasei moduliu n. Įrodysime, kad teisinga ir atvirkščia priklausomybė: bet kuris liekanų klasės K_a moduliu n skaičius patenka į vieną (4.7) sekos liekanų klasę moduliu nk.

Jeigu $b\in K_a$, K_a – liekanų klasė moduliu n, tai

$$b=a+nt.$$

Padalykime t iš k su liekana:

$$t=sk+r,\ 0\leqslant r\leqslant k.$$

Tuomet

$$b=a+rn+skn$$

ir

$$b\equiv a+rn\ (\mathrm{mod}\ kn).$$

Liekanų klasė moduliu kn, kuriai priklauso liekana $a+rn$, $0\leqslant r\leqslant k-1$, yra iš (4.7) sekos.

Išvada. *Lyginio*

$$ax\equiv b\ (\mathrm{mod}\ m)$$

d *skirtingų sprendinių* (*kai* $d=(a,\ m)\mid b$) *sudaro vieną lyginio*

$$\frac{a}{d}\,x\equiv\frac{b}{d}\ \left(\mathrm{mod}\ \frac{m}{d}\right)$$

sprendinį. Ir atvirkščiai, naudojantis (4.5) *formulėmis, kiekvieną pastarojo lyginio sprendinį galima suskaidyti į* d *lyginio* $ax\equiv b$ (mod m) *sprendinių.*

Pavyzdžiai. 1. Lyginys

$$45x\equiv 18\ (\mathrm{mod}\ 21)$$

turi 3 sprendinius, nes $(45,\ 21)=3$ ir $3\mid 18$. Vienas iš šio lyginio sprendinių yra K_6. Kitus sprendinius gausime didindami liekanų klasės K_6 numerį skaičiais $m/d=21/3=7$. Taigi kiti sprendiniai yra K_{13} ir K_{20}.

2. Suskaidysime liekanų klasę K_1 moduliu 7 į 5 liekanų klases moduliu 35. Pasirėmę 59 teoremos formulėmis, gauname šias liekanų klases:

$$K_1,\ K_8,\ K_{15},\ K_{22},\ K_{29}.$$

Pirmojo laipsnio lyginių sprendimo būdai. Išnagrinėsime keletą pirmojo laipsnio lyginių sprendimo būdų. Vienas iš jų, vadinamas *Oilerio būdu*, paremtas šia teorema.

60 teorema. *Jeigu* $(a, m)=1$, *tai lyginio*

$$ax \equiv b \pmod m$$

sprendinys yra liekanų klasė

$$x \equiv a^{\varphi(m)-1} b \pmod m. \tag{4.8}$$

Įrodymas. Į lyginį $ax \equiv b \pmod m$ vietoj x įrašę skaičių $a^{\varphi(m)-1} b$, gauname

$$a^{\varphi(m)} b \equiv b \pmod m.$$

Kadangi $(a, m)=1$, tai pagal Oilerio teoremą

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Todėl gauname teisingą lyginį

$$b \equiv b \pmod m.$$

Remdamiesi šia bei 59 teoremomis, galime išspręsti bet kurį pirmojo laipsnio lyginį.

Nurodysime kai kuriuos pirmojo laipsnio lyginių sprendimo būdus.

1. Tarkime, kad

$$ax \equiv b \pmod m$$

ir $d=(a, m) \mid b$. Padaliję to lyginio narius ir modulį m iš d, gauname lyginį

$$\frac{a}{d}\, x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right).$$

Kadangi skaičiai a/d ir b/d yra sveikieji ir tarpusavyje pirminiai, tai pastarojo lyginio sprendinį galima rasti iš (4.8) formulės. Jeigu K_c yra to lyginio sprendinys moduliu m/d, tai pagal 59 teoremą jį galima suskaidyti į d skirtingų liekanų klasių, kurios bus lyginio $ax \equiv b \pmod m$ sprendiniai.

2. Taikydami Euklido algoritmą, galime rasti sveikuosius neapibrėžtosios lygties

$$ax + mt = b$$

sprendinius, kai $(a, m) \mid b$. Jeigu x_0 ir t_0 yra skaičių, tenkinančių tą lygtį, pora, tai K_{x_0} yra lyginio $ax \equiv b \pmod m$ sprendinys, nes iš lygybės

$$ax_0 + mt_0 = b$$

išplaukia lyginys

$$ax_0 \equiv b \pmod m.$$

Taikant Euklido algoritmą, galima naudotis skaičių a ir m didžiausio bendrojo daliklio tiesinės išraiškos radimo būdais.

3. Ieškant neapibrėžtosios lygties

$$ax+mt=b, \quad (a, m)=1,$$

sprendinių, galima remtis 45 teoremos formulėmis. Iš jų išplaukia, kad lyginio $ax\equiv b \pmod m$ sprendinys yra liekanų klasė K_{x_0} moduliu m; čia

$$x_0=(-1)^{k-1}b\cdot Q_{k-1}, \tag{4.9}$$

Q_{k-1} yra trupmenos a/m skleidinio grandinine trupmena priešpaskutinio redukto (jo numeris $k-1$) vardiklis.

4. Lyginį $ax\equiv b \pmod m$ pavyksta išspręsti ir atliekant elementariuosius pertvarkius, kuriais jo koeficientai pakeičiami mažesniais skaičiais. Vienas iš tokių būdų – pridėti prie b tokį modulio kartotinį, kad suma dalytųsi iš a. Padaliję abi lyginio puses iš a, randame vienintelį lyginio sprendinį moduliu m, kai $(a, m)=1$. Tačiau jeigu $(a, m)=d>1$, tai, dalydami abi lyginio puses iš d, modulį taip pat turime dalyti iš (m, a). Gautasis sprendinys yra liekanų klasė moduliu $m/(a, m)$, kurią galime suskaidyti į (a, m) liekanų klasių moduliu m.

5. Reikia prisiminti ir patį primityviausią lyginių (ne tik pirmojo laipsnio) sprendimo būdą – patikrinti visų m liekanų klasių atstovus ir nustatyti, kurios klasės yra sprendiniai. Tas būdas patogus, kai modulis yra nedidelis skaičius.

Pirmojo laipsnio lyginių sprendimo pavyzdžiai. Išspręsime pavyzdį pirmaisiais 4 būdais. Rasime visus lyginio

$$45x\equiv 57 \pmod{69} \tag{4.10}$$

sprendinius.

Kadangi $(45, 69)=3$ ir $3/57$, tai lyginys turi 3 sprendinius moduliu 69.

1. Dalijame lyginį iš 3:

$$15x\equiv 19 \pmod{23}.$$

Pagal (4.8) formulę sprendinys moduliu 23 yra liekanų klasė

$$x\equiv 15^{\varphi(23)-1}\cdot 19 \pmod{23},$$

$$x\equiv 15^{21}\cdot 19 \pmod{23}.$$

Kadangi

$$15\equiv -8 \pmod{23},$$

tai

$$15^2\equiv 64\equiv -5 \pmod{23},$$

$$15^4\equiv (-5)^2\equiv 2 \pmod{23},$$

$$15^{20}\equiv 2^5\equiv 9 \pmod{23},$$

$$15^{21}\equiv 9\cdot 15\equiv -3 \pmod{23},$$

$$15^{21}\cdot 19\equiv -57\equiv 12 \pmod{23}.$$

Radome

$$x\equiv 15^{21}\cdot 19\equiv 12 \pmod{23}.$$

Tą liekanų klasę moduliu 23 galima suskaidyti į 3 liekanų klases moduliu 69:

$$x_1 \equiv 12 \pmod{69}.$$

$$x_2 \equiv 35 \pmod{69},$$

$$x_3 \equiv 58 \pmod{69}.$$

Taigi skaičiai 12, 35, 58 yra iš trijų liekanų klasių moduliu 69. Tos klasės yra (4.10) lyginio sprendiniai.

2. Skaičiams 45 ir 69 taikome Euklido algoritmą:

$$45 = 69 \cdot 0 + 45,$$

$$69 = 45 \cdot 1 + 24,$$

$$45 = 24 \cdot 1 + 21,$$

$$24 = 21 \cdot 1 + 3,$$

$$21 = 3 \cdot 7.$$

Paskutinė nelygi nuliui algoritmo liekana r_3 lygi 3 (čia vartojame tą pačią numeravimo sistemą kaip ir Euklido algoritmo apibrėžime, (1.7) lygybėse pirmoji liekana žymima r, antroji — r_1 ir t. t.). Iš (1.9) formulės, aprašančios paskutinę skaičių a ir b Euklido algoritmo nenulinę liekaną — tų skaičių d. b. d. tiesinę išraišką (§ 4), gauname

$$r_3 = 3 = (-1)^3 45 \cdot \big((1, 1, 1)\big) + (-1)^4 69 \cdot \big((0, 1, 1, 1)\big).$$

Sudarę Oilerio skliaustų skaičiavimo lentelę

	0	1	1	1
$\big((q_0, q_1, q_2, q_3)\big)$	0	1	1	2
$\big((q_1, q_2, q_3)\big)$		1	2	3

randame $\big((1, 1, 1)\big) = 3$, $\big((0, 1, 1, 1)\big) = 2$. Todėl

$$3 = -45 \cdot 3 + 69 \cdot 2.$$

Padauginę abi šios tapatybės puses iš 19, turime

$$45 \cdot (-57) + 69 \cdot 38 = 57.$$

Ši lygybė ekvivalenti lyginiui

$$45 \cdot (-57) \equiv 57 \pmod{69}.$$

Taigi skaičius $x_0 = -57$ priklauso sprendiniui moduliu 69. Šis skaičius yra iš liekanų klasės K_{12} tuo moduliu.

Kitas liekanų klases — sprendinius nustatome taip pat kaip ir pirmuoju atveju, t. y. remdamiesi 59 teorema.

3. Išskleidžiame skaičių 45/69 grandinine trupmena. Jos elementai yra skaičių 45 ir 69 Euklido algoritmo nepilnieji santykiai. Juos radome nagrinėdami antrąjį atvejį. Todėl

$$\frac{45}{69} = [0, 1, 1, 1, 7].$$

Sudarysime lentelę reduktams apskaičiuoti:

i	-1	0	1	2	3	4
q_i	1	0	1	1	1	7
P_i	1	0	1	1	2	15
Q_i	0	1	1	2	3	23

Lentelę surašėme visą, nors šiuo atveju pakaktų ir jos dalies. Lentelėje matome, kad paskutinis gautasis reduktas R_4 sutampa su skaičiumi 45/69, suprastintu iš 3. Be to, pastebime, kad praeitame pavyzdyje sudaryta Oilerio skliaustų skaičiavimo lentelė yra šios lentelės dalis. Trupmenos 45/69 priešpaskutinio redukto R_3 vardiklis Q_3 lygus 3. Pagal (2.3a) formules Q_3 lygus Oilerio skliaustams ((1, 1, 1)). Pasirėmę (4.9) formule, randame skaičių x_0, tenkinantį (4.10) lyginį:

$$x_0=(-1)^3 19\cdot 3.$$

(4.9 formulė taikoma tik suprastintajai lygčiai

$$\frac{a}{(a,\ m)}\ x+\frac{m}{(a,\ m)}\ t=\frac{b}{(a,\ m)}\cdot\ )$$

Gautasis skaičius $x_0=-57$ yra toks pat kaip ir antruoju atveju, tik jis priklauso liekanų klasei K_{12} moduliu 23, nes suprastintoji lygtis yra $15x+23t=19$. Belieka šią liekanų klasę suskaidyti į 3 liekanų klases moduliu 69.

4. Lyginį pertvarkome remdamiesi tuo, kad prie bet kurios lyginio pusės galime pridėti modulio kartotinį:

$$15x\equiv 19 \pmod{23},$$

$$15x\equiv 19+23 \pmod{23},$$

$$15x\equiv 42 \pmod{23},$$

$$5x\equiv 14 \pmod{23}.$$

$$5x\equiv 14+2\cdot 23 \pmod{23},$$

$$5x\equiv 60 \pmod{23},$$

$$x\equiv 12 \pmod{23}.$$

Taigi vėl gauname tą patį sprendinį moduliu 23.

Pažymėsime, kad visais būdais, išskyrus trečiąjį, galime spręsti ir suprastintus lyginius

$$ax\equiv b \pmod{m},$$

kai $(a, m)=1$, ir nesuprastintus lyginius, kai $(a, m)>1$. Sprendžiant trečiuoju būdu, visus lyginio narius reikia dalyti iš (a, m).

Uždaviniai

4. Suskaidykite liekanų klasę $x\equiv 3 \pmod 8$ į liekanų klases moduliais 16, 24, 32, 40, 48.

5. Išspręskite pirmojo laipsnio lyginius:

1) $5x\equiv 1 \pmod 7$;
2) $9x\equiv 10 \pmod{11}$;
3) $11x\equiv 3 \pmod{13}$;
4) $13x\equiv 5 \pmod{15}$;
5) $17x\equiv 50 \pmod{19}$;
6) $20x\equiv 7 \pmod{27}$;
7) $27x\equiv 2 \pmod{31}$;
8) $31x\equiv 100 \pmod{37}$.

6. Išspręskite pirmojo laipsnio lyginius naudodamiesi grandininėmis trupmenomis:

1) $37x \equiv 16 \pmod{47}$;
2) $25x \equiv 32 \pmod{53}$;
3) $61x \equiv 31 \pmod{67}$;
4) $67x \equiv 2 \pmod{71}$;
5) $50x \equiv 1 \pmod{73}$;
6) $59x \equiv 49 \pmod{79}$;
7) $61x \equiv 12 \pmod{83}$;
8) $42x \equiv 59 \pmod{89}$.

7. Raskite visus pirmojo laipsnio lyginių sprendinius:

1) $18x \equiv 16 \pmod{22}$;
2) $33x \equiv 9 \pmod{39}$;
3) $52x \equiv 28 \pmod{60}$;
4) $74x \equiv 32 \pmod{94}$;
5) $34x \equiv 24 \pmod{38}$;
6) $60x \equiv 33 \pmod{84}$;
7) $54x \equiv 26 \pmod{62}$;
8) $50x \equiv 20 \pmod{70}$.

8. Nustatykite, kurie šių kreivių taškai yra sveikieji:

1) $15y = 2x^3 - 5x^2 + 4x + 11$, kai $-2 < x < 8$;
2) $14y = 3x^3 - 4x^2 + 11x + 4$, kai $-7 < x < 7$.

9. Prirašykite prie skaičiaus 523 iš dešinės tokius tris skaitmenis, kad gautasis skaičius dalytųsi iš 7, 8, 9.

10. Išspręskite lyginį $x^2 - 4x + 3 \equiv 0 \pmod 6$ remdamiesi būtinąja sąlyga $x^2 - 4x + 3 \equiv 0 \pmod 2$.

§36. Lyginių sistemos

Įrodysime keletą bendrų dėsnių apie lyginių sistemas. Šiame paragrafe nagrinėsime lyginius, šiek tiek bendresnius už tuos, kuriuos praktiškai spręsime.

61 teorema. *Jeigu* $m_1, m_2, \ldots, m_k$ *yra poromis tarpusavyje pirminiai skaičiai, tai lyginys*

$$f(x) \equiv 0 \pmod{m_1 m_2 \ldots m_k} \tag{4.11}$$

ekvivalentus lyginių sistemai

$$\begin{aligned} &f(x) \equiv 0 \pmod{m_1}, \\ &f(x) \equiv 0 \pmod{m_2}, \\ &\cdots\cdots\cdots\cdots \\ &f(x) \equiv 0 \pmod{m_k}; \end{aligned} \tag{4.12}$$

čia $f(x)$ *— polinomas su sveikaisiais koeficientais.*

Įrodymas. Jeigu x_0 tenkina (4.11) lyginį, tai $f(x_0)$ dalijasi iš sandaugos $m_1 m_2 \ldots m_k$. Tačiau tada $f(x_0)$ dalijasi ir iš kiekvieno dauginamojo m_s:

$$\bigwedge_{s=1}^{k} f(x_0) \equiv 0 \pmod{m_s}.$$

Taigi x_0 tenkina (4.12) lyginių sistemą.

Lengvai įsitikiname, kad teisingas ir atvirkščias teiginys. Iš tikrųjų, jeigu x_0 tenkina bet kurį (4.12) sistemos lyginį, tai $f(x_0)$ dalijasi iš visų skaičių $m_1, m_2, \ldots, m_k$, kartu ir iš jų sandaugos, nes tie skaičiai poromis tarpusavyje pirminiai (pagal 12 teoremos išvadą).

Teorema įrodyta.

Sistemos

$$f_1(x) \equiv 0 \pmod{m_1},$$
$$f_2(x) \equiv 0 \pmod{m_2},$$
$$\cdots\cdots\cdots\cdots$$
$$f_k(x) \equiv 0 \pmod{m_k}, \tag{4.13}$$

kurios moduliai poromis tarpusavyje pirminiai skaičiai, sprendinys yra liekanų klasė moduliu

$$M = m_1 m_2 \ldots m_k. \tag{4.14}$$

Jos skaičiai tenkina visus sistemos lyginius.

62 teorema. *Jeigu* (4.13) *sistemos, kurios moduliai yra poromis tarpusavyje pirminiai skaičiai, lyginiai turi atitinkamai* T_1, T_2, ..., T_k *sprendinių, tai sistemos sprendinių skaičius lygus sandaugai*

$$T_1 T_2 \ldots T_k.$$

Įrodymas. Skaičius M_i, $\overline{M}_i$ ($i = 1, 2, \ldots, k$) apibrėšime šitaip:

$$M_i = \frac{M}{m_i},$$

$$M_i \overline{M}_i \equiv 1 \pmod{m_i}. \tag{4.15}$$

Imkime po vieną kiekvieno (4.13) sistemos lyginio sprendinį

$$x \equiv b_1 \pmod{m_1},$$
$$x \equiv b_2 \pmod{m_2},$$
$$\cdots\cdots\cdots\cdots$$
$$x \equiv b_k \pmod{m_k}$$

ir sudarykime skaičių

$$x_0 = b_1 M_1 \overline{M}_1 + b_2 M_2 \overline{M}_2 + \ldots + b_k M_k \overline{M}_k;$$

čia $\overline{M}_i$ – bet kurie skaičiai, tenkinantys (4.15) lyginį.

Įrodysime, kad skaičius x_0 tenkina bet kurį (4.13) sistemos lyginį, pavyzdžiui,

$$f_1(x) \equiv 0 \pmod{m_1}. \tag{4.16}$$

Pagal skaičių M_i apibrėžimą visi jie, išskyrus M_1, dalijasi iš m_1. Vadinasi,

$$x_0 \equiv b_1 M_1 \overline{M}_1 \pmod{m_1}.$$

Naudodamiesi (4.15) lyginiu, randame

$$x_0 \equiv b_1 \pmod{m_1}.$$

Tačiau b_1 yra skaičius, priklausantis liekanų klasei, kuri yra (4.16) lyginio sprendinys. Vadinasi, x_0 tenkina tą lyginį.

Skaičius x_0 sudarytas paėmus po vieną visų sistemos lyginių sprendinį. Tačiau pirmasis sistemos lyginys pagal teoremos sąlygą turi T_1 sprendinių. Vadinasi, skaičių b_1 galima parinkti T_1 būdų – iš visų skirtingų moduliu m_1 klasių, kurios yra to lyginio sprendiniai. Analogiškai skaičių b_2 galima parinkti T_2 būdų. Visi tie skaičiai b_2 tarpusavyje nelygsta moduliu m_2 ir t. t. Vadinasi, skaičių x_0 galima sudaryti $T_1T_2 \ldots T_k$ skirtingų būdų. Visos taip sudarytos x_0 reikšmės tarpusavyje nelygsta moduliu M.

Tarkime priešingai,

$$x_0 = b_1 M_1 \overline{M}_1 + b_2 M_2 \overline{M}_2 + \ldots + b_k M_k \overline{M}_k,$$

$$x_0' = b_1' M_1 \overline{M}_1 + b_2' M_2 \overline{M}_2 + \ldots + b_k' M_k \overline{M}_k,$$

ir

$$\bigvee_{s=1}^{k} b_s \not\equiv b_s' \pmod{m_s},$$

$$x_0 \equiv x_0' \pmod{M}.$$

Pastarasis lyginys ekvivalentus sistemai

$$\begin{cases} x \equiv x_0' \pmod{m_1}, \\ x \equiv x_0' \pmod{m_2}, \\ \cdots\cdots\cdots\cdots \\ x \equiv x_0' \pmod{m_k}. \end{cases}$$

Imame bet kurį tos sistemos lyginį

$$x_0 \equiv x_0' \pmod{m_i}$$

ir vietoj x_0 ir x_0' įrašome jų reikšmes. Visai taip pat kaip ir teoremos įrodymo pradžioje gauname

$$b_i M_i \overline{M}_i \equiv b_i' M_i \overline{M}_i \pmod{m_i}$$

$$b_i \equiv b_i' \pmod{m_i}$$

su visais indeksais i, $1 \leqslant i \leqslant k$. Tačiau tai prieštarauja prielaidai, kad bent vienos poros skaičiai b_i, b_i' nelygsta moduliu m_i. Teorema įrodyta.

Pirmojo laipsnio lyginių sistemos sprendimas. Nagrinėsime pirmojo laipsnio lyginių sistemas

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1}, \\ a_2 x \equiv b_2 \pmod{m_2}, \\ \cdots\cdots\cdots\cdots \\ a_k x \equiv b_k \pmod{m_k}, \end{cases} \tag{4.17}$$

kuriose moduliai m_1, m_2, ..., m_k yra poromis tarpusavyje pirminiai skaičiai. Tokią sistemą galime spręsti dvejopai: *nuosekliuoju būdu* arba naudodamiesi 62 teoremos formulėmis.

Nagrinėsime nuoseklųjį lyginių sprendimo būdą.

Pavyzdys. Išspręsime sistemą

$$\begin{cases} 10x \equiv 1 \pmod{13}, \\ 8x \equiv 10 \pmod{18}, \\ 6x \equiv 5 \pmod{23}. \end{cases}$$

Sprendžiame vieną kurį nors tos sistemos lyginį, pavyzdžiui, pirmąjį, bet kuriuo iš žinomų pirmojo laipsnio lyginių sprendimo būdų:

$$10x \equiv 1 \pmod{13},$$

$$10x \equiv 1 + 3 \cdot 13 \pmod{13},$$

$$10x \equiv 40 \pmod{13},$$

$$x \equiv 4 \pmod{13}.$$

To lyginio sprendinį sudaro visi

$$x = 4 + 13t, \quad t \in \mathbf{Z}, \tag{4.18}$$

pavidalo skaičiai. Parenkame t taip, kad (4.18) pavidalo skaičiai kartu būtų ir kitų sistemos lyginių sprendinių skaičiai.

(4.18) x išraišką įrašome į bet kurį kitą sistemos lyginį, pavyzdžiui, į antrąjį:

$$8x \equiv 10 \pmod{18},$$

$$8(4 + 13t) \equiv 10 \pmod{18},$$

$$32 + 104t \equiv 10 \pmod{18},$$

$$104t \equiv -22 \pmod{18},$$

$$14t \equiv -22 \pmod{18}.$$

Tas lyginys turi du sprendinius, nes $(14, 18) = 2$ ir $2 \mid -22$:

$$14t \equiv -22 \pmod{18},$$

$$7t \equiv -11 \pmod{9},$$

$$7t \equiv -11 + 2 \cdot 9 \pmod{9},$$

$$7t \equiv 7 \pmod{9},$$

$$t \equiv 1 \pmod{9}.$$

Gautasis lyginys reiškia, kad

$$t = 1 + 9t_1: \tag{4.19}$$

čia t_1 – bet kuris sveikasis skaičius. Įrašę t išraišką į (4.18), randame

$$x = 4 + 13t = 4 + 13(1 + 9t_1), \quad x = 17 + 117t_1.$$

Skaičiai x tenkina pirmuosius du sistemos lyginius. Kad tie skaičiai tenkintų trečiąjį sistemos lyginį, turime juos įrašyti į tą lyginį. Įrašę gauname

$$6x \equiv 5 \pmod{23},$$

$$6(17 + 117t_1) \equiv 5 \pmod{23},$$

$$102 + 702t_1 \equiv 5 \pmod{23},$$

$$702t_1 \equiv -97 \pmod{23},$$

$$12t_1 \equiv -5 \pmod{23},$$

$$12t_1 \equiv -5+7\cdot 23 \pmod{23},$$

$$12t_1 \equiv 156 \pmod{23},$$

$$t_1 \equiv 13 \pmod{23}.$$

Taigi

$$t_1 = 13+23t_2;$$

čia t_2 – bet kuris sveikasis skaičius. Įrašę t_1 reikšmę į (4.19), gauname

$$x = 17+117t_1 = 17+117(13+23t_2),$$

$$x = 1538+117\cdot 23t_2,$$

$$x = 1538+13\cdot 9\cdot 23t_2.$$

Tokio pavidalo skaičiai x sudaro liekanų klasę

$$x \equiv 1538 \pmod{13\cdot 9\cdot 23}.$$

Visi jie yra pradinės lyginių sistemos sprendiniai. Tą liekanų klasę galime suskaidyti į dvi liekanų klases moduliu

$$13\cdot 18\cdot 23.$$

Pasirėmę 59 teorema, gauname

$$x_1 \equiv 1538 \pmod{13\cdot 18\cdot 23},$$

$$x_2 \equiv 4229 \pmod{13\cdot 18\cdot 23}.$$

Tos dvi klasės ir yra sistemos sprendiniai moduliu $13\cdot 18\cdot 23$. Pagal 62 teoremą atskirų lyginių sprendinių skaičius atitinkamai yra

$$T_1 = 1,\ T_2 = 2,\ T_3 = 1$$

ir sistemos sprendinių skaičius

$$T_1T_2T_3 = 2.$$

Jeigu lyginių sistemos moduliai yra poromis tarpusavyje pirminiai skaičiai, tai tą sistemą galime spręsti remdamiesi 61 teorema.

Nuosekliuoju sistemos sprendimo būdu galime spręsti ir sistemas, kurių moduliai turi bendrųjų daliklių. Tuomet nėra teisingas 62 teoremos teiginys dėl sprendinių skaičiaus.

Pavyzdys. Kiekvienas sistemos

$$5x \equiv 1 \pmod{8},$$

$$3x \equiv 2 \pmod{10}$$

lyginys turi po 1 sprendinį, tačiau sistema sprendinių neturi. Iš tikrųjų nesunku įsitikinti, kad liekanų klasė

$$x \equiv 5 \pmod{8}$$

yra pirmojo sistemos lyginio sprendinys, tačiau nė vienas tos klasės skaičius netenkina antrojo lyginio.

Uždaviniai

11. Išspręskite pirmojo laipsnio lyginių sistemas keitimo bei 62 teoremoje nurodytu būdu:

1) $\begin{cases} 3x \equiv 1 \pmod{11}, \\ 5x \equiv 2 \pmod{13}, \\ 7x \equiv 3 \pmod{15}; \end{cases}$ 3) $\begin{cases} 12x \equiv 15 \pmod{17}, \\ 10x \equiv 4 \pmod{19}, \\ 21x \equiv 16 \pmod{23}; \end{cases}$ 5) $\begin{cases} 5x \equiv 1 \pmod{23}, \\ 15x \equiv 11 \pmod{43}, \\ 25x \equiv 21 \pmod{63}; \end{cases}$

2) $\begin{cases} x \equiv 5 \pmod{7}, \\ 5x \equiv 7 \pmod{9}, \\ 7x \equiv 9 \pmod{11}; \end{cases}$ 4) $\begin{cases} 2x \equiv 10 \pmod{18}, \\ 7x \equiv 1 \pmod{19}, \\ x \equiv 13 \pmod{23}; \end{cases}$ 6) $\begin{cases} 5x \equiv 1 \pmod{41}, \\ 5x \equiv 1 \pmod{51}, \\ 5x \equiv 1 \pmod{61}. \end{cases}$

§37. Lyginiai moduliais, lygiais pirminio skaičiaus laipsniui

Lyginių

$$f(x) \equiv 0 \pmod{m}$$

sprendimą detaliai nagrinėjame tuo atveju, kai $f(x)$ yra pirmojo laipsnio polinomas. Jeigu $f(x)$ laipsnis didesnis už 1, tai lyginių teorija ir jų sprendimo metodai žymiai sudėtingesni.

Jeigu skaičiaus m kanoninis skaidinys yra

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

tai, remdamiesi 61 teorema, lyginį $f(x) \equiv 0 \pmod{m}$ galime pakeisti jam ekvivalenčia sistema

$$\begin{aligned} &f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ &f(x) \equiv 0 \pmod{p_2^{\alpha_2}}, \\ &\cdots\cdots\cdots\cdots \\ &f(x) \equiv 0 \pmod{p_k^{\alpha_k}}. \end{aligned}$$

Norėdami išspręsti tokią sistemą, turime mokėti spręsti lyginius

$$f(x) \equiv 0 \pmod{p^{\alpha}},$$

kurių modulis yra pirminio skaičiaus natūrinis laipsnis. Nagrinėsime tokių lyginių sprendimą.

Jeigu $f(x)$ yra polinomas su sveikaisiais koeficientais, p^{α} — pirminio skaičiaus natūrinis laipsnis, tai lyginys

$$f(x) \equiv 0 \pmod{p^{\alpha}}$$

turi tiek sprendinių, kiek yra lyginio

$$f(x) \equiv 0 \pmod{p}$$

sprendinių

$$x \equiv x_0 \pmod{p},$$

tenkinančių sąlygą

$$p \nmid f'(x_0). \tag{4.20}$$

Įrodymas. Lyginį $x \equiv x_0 \pmod p$ keičiame lygybe

$$x = x_0 + pt. \tag{4.21}$$

Tie skaičiai x tenkina lyginį

$$f(x) \equiv 0 \pmod p,$$

kai t – bet kuris sveikasis skaičius.

Rasime, kokie turi būti sveikieji skaičiai t, kad (4.21) pavidalo skaičiai x būtų lyginio

$$f(x) \equiv 0 \pmod{p^2}$$

sprendiniai. Vietoj x į tą lyginį įrašę sumą $x_0 + pt$ ir išskleidę polinomą $f(x)$ Teiloro eilute, gauname

$$f(x) = f(x_0 + pt) =$$

$$= f(x_0) + ptf'(x_0) + \frac{p^2 t^2}{2} f''(x_0) + \ldots \equiv 0 \pmod{p^2}. \tag{4.22}$$

Bet kurio polinomo su sveikaisiais koeficientais k-osios išvestinės visi koeficientai dalijasi iš $k!$. Iš tikrųjų, jeigu

$$f(x) = \sum_{m=0}^{n} a_m x^m,$$

tai

$$f^k(x) = \sum_{m=k}^{n} a_m m(m-1)\ldots(m-k+1) x^{m-k},$$

tačiau

$$\frac{m(m-1)\ldots(m-k+1)}{k!} = C_m^k.$$

(4.22) lyginio dešiniojoje pusėje visi nariai, išskyrus galbūt du pirmuosius, yra p^2 kartotiniai. Taigi

$$f(x_0) + ptf'(x_0) \equiv 0 \pmod{p^2}.$$

Kadangi x tenkina lyginį $f(x) \equiv 0 \pmod p$, tai skaičius $f(x_0)$ dalijasi iš p. Lyginį moduliu p^2 padaliję iš p, gauname

$$f'(x_0)\, t \equiv -\frac{f(x_0)}{p} \pmod p.$$

Iš 4.20 sąlygos išplaukia, kad tas lyginys visuomet išsprendžiamas ir turi vieną sprendinį, kurį žymėsime

$$t \equiv y_0 \pmod p,$$

arba

$$t = y_0 + pt_1;$$

čia t_1 – bet kuris sveikasis skaičius. Įrašę t reikšmę į (4.21), gauname

$$x = x_0 + p(y_0 + pt_1).$$

Pažymėję

$$x_1 = x_0 + py_0,$$

turime

$$x = x_1 + p^2 t_1. \tag{4.23}$$

Visi (4.23) pavidalo skaičiai x, tarp jų ir x_1, tenkina lyginį

$$f(x) \equiv 0 \pmod{p^2}.$$

Parenkame t_1 taip, kad tie skaičiai x tenkintų ir lyginį

$$f(x) \equiv 0 \pmod{p^3}.$$

Į šį lyginį vietoj x įrašę jo (4.23) išraišką, $f(x)$ vėl skleidžiame Teiloro eilute:

$$f(x) = f(x_1 + p^2 t_1) = f(x_1) + p^2 t_1 f'(x_1) + \frac{p^4 t_1^2}{2} f''(x_1) + \ldots \equiv 0 \pmod{p^3}.$$

Gauname

$$f(x_1) + p^2 t_1 f'(x_1) \equiv 0 \pmod{p^3},$$

$$f'(x_1)\, t_1 \equiv -\frac{f(x_1)}{p^2} \pmod{p}. \tag{4.24}$$

Dešiniojoje lyginio pusėje esantis reiškinys yra sveikasis skaičius, nes x_1 tenkina lyginį $f(x_1) \equiv 0 \pmod{p^2}$. Įrodysime, kad

$$\big(f'(x_1),\ p\big) = 1.$$

Iš $f'(x_1) \equiv 0 \pmod{p}$ išplauktų, kad

$$f'(x_0) \equiv 0 \pmod{p},$$

nes $x_1 \equiv x_0 \pmod{p}$, bet tai prieštarauja (4.20) sąlygai.

Vadinasi, pirmojo laipsnio (4.24) lyginys t_1 atžvilgiu visuomet išsprendžiamas ir turi vieną sprendinį

$$t_1 = z_0 \pmod{p},$$

arba

$$t_1 = z_0 + pt_2.$$

Įrašę t_1 reikšmę į (4.23), gauname

$$x \equiv x_2 + p^3 t_2 \quad (x_2 = x_1 + p^2 z_0). \tag{4.25}$$

Tie skaičiai x jau yra lyginio

$$f(x) \equiv 0 \pmod{p^3}$$

sprendiniai. Tą procesą tęsdami toliau, rasime sąlygą, kurią turi tenkinti t_2, kad (4.25) skaičiai tenkintų lyginį

$$f(x) \equiv 0 \pmod{p^4}$$

ir t. t.

Taigi kiekvienam lyginio

$$f(x) \equiv 0 \pmod{p}$$

sprendiniui, tenkinančiam (4.20) sąlygą, galime rasti vieną lyginio

$$f(x) \equiv 0 \pmod{p^\alpha}$$

sprendinį, kai α – bet koks natūrinis skaičius.

Du sprendiniai moduliu p^α, kurie atitinka dvi skirtingas x_0 reikšmes moduliu p, negali sutapti, nes iš lyginio

$$x \equiv x' \pmod{p^\alpha}$$

išplaukia, kad

$$x \equiv x' \pmod{p}.$$

Šie samprotavimai leidžia suformuluoti tokią išvadą.

Išvada. *Lyginio*

$$f(x) \equiv 0 \pmod{p^\alpha}$$

sprendinį

$$x \equiv x_{\alpha-1} \pmod{p^\alpha}$$

galime rasti iš formulių

$$f'(x_0)\, t_0 \equiv -\frac{f(x_0)}{p} \pmod{p},$$

$$f'(x_1)\, t_1 \equiv -\frac{f(x_1)}{p^2} \pmod{p},$$

$$f'(x_2)\, t_2 \equiv -\frac{f(x_2)}{p^3} \pmod{p},$$

$$\dots\dots\dots\dots\dots\dots$$

$$f'(x_{\alpha-2})\, t_{\alpha-2} \equiv -\frac{f(x_{\alpha-2})}{p^{\alpha-1}} \pmod{p},$$

$$x_k = x_{k-1} + p^k y_{k-1}, \quad 1 \leqslant k \leqslant \alpha - 2;$$

čia y_k – *toks fiksuotas skaičius, kad*

$$t_k \equiv y_k \pmod{p},$$

o x_0 – *lyginio* $f(x) \equiv 0 \pmod{p}$ *sprendinio skaičius, tenkinantis sąlygą* $p \nmid f'(x_0)$.

Pavyzdys. Išspręsime lyginį

$$3x^2+x+1\equiv 0 \pmod{125}.$$

Lyginio $3x^2+x+1\equiv 0 \pmod 5$ sprendinys yra klasė

$$x\equiv 1 \pmod 5.$$

Kadangi $5\nmid f'(1)=7$, tai sprendinių moduliais 5^2 ir 5^3 ieškome nuosekliai naudodamiesi išvados formulėmis.

Gauname lyginį

$$7t_0\equiv -1 \pmod 5,$$

$$t_0\equiv 2 \pmod 5.$$

Taigi $y_0=2$, $x_1=x_0+py_0=1+5\cdot 2=11$.

Toliau ieškome t_1:

$$f'(11)t_1\equiv -\frac{f(11)}{25} \pmod 5,$$

arba

$$67t_1\equiv 15 \pmod 5,$$

$$t_1\equiv 0 \pmod 5.$$

Vadinasi, $y_1=0$, $x_2=x_1$. Pradinio lyginio vienas iš sprendinių yra

$$x\equiv x_2 \pmod{5^3},$$

$$x\equiv 11 \pmod{125}.$$

Lyginys $3x^2+x+1\equiv 0 \pmod 5$ turi ir kitą sprendinį. Jį galime rasti tikrindami visų 5 liekanų klasių atstovus. Randame

$$x\equiv 2 \pmod 5.$$

Tas sprendinys tenkina ir (4.20) sąlygą. Analogiškai spręsdami, gauname kitą lyginio $3x^2+x+1\equiv 0 \pmod{125}$ sprendinį:

$$x\equiv -53 \pmod{125}.$$

Taigi lyginys

$$3x^2+x+1\equiv 0 \pmod{125}$$

turi du sprendinius – liekanų klases

$$x\equiv 11 \bmod (125),$$

$$x\equiv -53 \pmod{125}.$$

Uždaviniai

12. Išspręskite šiuos lyginius:

1) $2x^2-x-4\equiv 0 \pmod{27}$; 4) $x^3-2x+1\equiv 0 \pmod{125}$;

2) $x^3-5x^2+1\equiv 5 \pmod{81}$; 5) $x^3+x^2+2\equiv 0 \pmod{49}$;

3) $5x^2+2x+6\equiv 0 \pmod{25}$; 6) $x^4-x^3+x^2-1\equiv 0 \pmod{49}$.

§38. Lyginiai pirminiu moduliu

Praeitame paragrafe išdėstytas lyginių

$$f(x)\equiv 0 \pmod{p^\alpha}$$

sprendimo metodas paremtas tuo, kad yra žinomas lyginio

$$f(x)\equiv 0 \pmod p$$

sprendinys. Vadinasi, norint išspręsti lyginį sudėtiniu moduliu, reikia mokėti spręsti lyginius visais pirminiais moduliais. Deja, nėra jokių specifinių tokių lyginių sprendimo metodų, kai $f(x)$ – bet kurio laipsnio polinomas.

Nagrinėsime kai kurias lyginių pirminiu moduliu savybes.

63 teorema. *Kiekvieną lyginį*

$$f(x) \equiv 0 \pmod{p}$$

galima pakeisti ekvivalenčiu lyginiu

$$g(x) \equiv 0 \pmod{p},$$

kuriame polinomo laipsnis mažesnis už $p-1$.

Įrodymas. Tarkime, kad

$$f(x) = \sum_{k=0}^{n} a_k x^k.$$

Kiekvieną kintamojo x rodiklį k, ne mažesnį už p, padalykime su liekana iš $p-1$:

$$k = (p-1)q_k + r_k, \quad 0 \leqslant r_k < p-1.$$

Tada

$$x^k = (x^{p-1})^{q_k} \cdot x^{r_k}. \tag{4.26}$$

Jeigu $x \not\equiv 0 \pmod{p}$, tai iš Ferma teoremos išplaukia, kad

$$x^{p-1} \equiv 1 \pmod{p},$$

todėl

$$x^k \equiv x^{r_k} \pmod{p}.$$

Gauname

$$\sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{p-2} a_k x^k + \sum_{k=p-1}^{n} a_k x^k \equiv \sum_{k=0}^{p-2} a_k x^k + \sum_{k=p-1}^{n} a_k x^{r_k} \pmod{p}.$$

Pažymėję dešiniojoje lyginio pusėje esantį polinomą $g(x)$, matome, kad teoremos tvirtinimas teisingas, kai $(x, p) = 1$.

Jeigu x dalijasi iš p, tai iš p dalijasi ir visi dėmenys $a_k x^k$, kai $k > 0$. Tuomet

$$f(x) \equiv a_0 \pmod{p}.$$

Vadinasi, ir šiuo atveju teoremos tvirtinimas teisingas.

Praktiškai žeminant polinomo laipsnį, patogu remtis ir 55 teorema (su visais x $x^p \equiv x \pmod{p}$).

Pavyzdžiai. 1. Lyginį

$$1021x^{373} + 15x^{13} + 80x \equiv 10 \pmod{37}$$

pakeisime ekvivalenčiu žemesnio laipsnio lyginiu.

$$373 = 10 \cdot 37 + 3,$$

todėl

$$x^{373}=(x^{37})^{10}x^3\equiv x^{10+3}\equiv x^{13}\pmod{37}.$$

Taigi

$$1021x^{373}+15x^{13}\equiv 22x^{373}+15x^{13}\equiv 37x^{13}\equiv 0\pmod{37}.$$

Kadangi $80\equiv 6\pmod{37}$, tai

$$6x\equiv 10\pmod{37}.$$

2. Išspręsime lyginį

$$2x^{21}+3x^{20}+3x^{16}+x^5-x+8\equiv 0\pmod 5.$$

Remdamiesi įrodyta teorema, to lyginio kairiojoje pusėje esantį polinomą, dalydami jį iš x^5-x, galime pakeisti ne aukštesnio kaip ketvirtojo laipsnio polinomu. Paprasčiau gausime rezultatą x^5 visur pakeitę x moduliu 5:

$$x^{21}=(x^5)^4x\equiv x^4\cdot x\equiv x^5\equiv x\pmod 5,$$

$$x^{20}=(x^5)^4\equiv x^4\pmod 5,$$

$$x^{16}=(x^5)^3x\equiv x^4\pmod 5.$$

Gauname lyginį:

$$2x+3x^4+3x^4+x-x+8\equiv 0\pmod 5,$$

$$6x^4+2x+8\equiv 0\pmod 5,$$

$$x^4+2x+3\equiv 0\pmod 5.$$

Kadangi 5 yra pirminis skaičius, tai moduliu 5 tik viena liekanų klasė K_0 nėra tarpusavyje pirminė su 5. Nesunku įsitikinti, kad ta klasė nėra sprendinys. Kitų liekanų klasių atstovai yra tarpusavyje pirminiai su moduliu, jiems teisinga Ferma teorema

$$x^4\equiv 1\pmod 5.$$

Taigi sprendžiamasis lyginys pakeičiamas šitokiu:

$$1+2x+3\equiv 0\pmod 5,$$

$$2x\equiv -4\pmod 5,$$

$$x\equiv -2\pmod 5.$$

Tai ir yra vienintelis lyginio sprendinys.

Suformuluosime be įrodymo teoremą apie lyginio pirminiu moduliu p sprendinių skaičių.

64 teorema. *Jeigu* $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ *yra polinomas su sveikaisiais koeficientais ir*

$$(a_n,\ p)=1,$$

tai lyginio

$$f(x)\equiv 0\pmod p$$

sprendinių skaičius N *tenkina nelygybę*

$$N\leqslant \min(n,\ p-1).$$

Iš šios teoremos išplaukia viena įdomi lyginių savybė.

Pažymėkime $\deg f(x)$ polinomo $f(x)$ laipsnį.

65 teorema. *Jeigu lyginio*

$$f(x)\equiv 0\,(\mathrm{mod}\,p)$$

sprendinių skaičius didesnis už $n=\deg f(x)$, *tai visi polinomo* $f(x)$ *koeficientai dalijasi iš* p.

Įrodymas. Jeigu $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ ir $(a_n,\ p)=1$, tai lyginys

$$f(x)\equiv 0\,(\mathrm{mod}\,p) \tag{4.27}$$

turi ne daugiau kaip n sprendinių. Kadangi sprendinių yra daugiau kaip n, tai a_n yra modulio p kartotinis, ir (4.27) lyginys ekvivalentus lyginiui

$$a_{n-1}x^{n-1}+\ldots+a_1x+a_0\equiv 0\,(\mathrm{mod}\,p).$$

To lyginio sprendinių skaičius lygus (4.27) lyginio sprendinių skaičiui ir todėl yra didesnis už polinomo laipsnį, t. y. už $n-1$. Vadinasi, vyriausiasis koeficientas a_{n-1} vėl dalijasi iš p ir tą narį lyginyje galima praleisti. Taip samprotaujant toliau, gaunamas teoremoje suformuluotas teiginys.

Iš 64 ir 65 teoremų galime gauti keletą sąryšių, kuriais remiantis nustatoma, ar skaičius yra pirminis, ar sudėtinis.

Įrodysime šitokią teoremą.

66 (Vilsono) teorema. *Jeigu* p *yra pirminis skaičius, tai*

$$(p-1)!+1\equiv 0\,(\mathrm{mod}\,p).$$

Įrodymas. Teorema teisinga, kai $p=2$. Kai $p>2$, nagrinėjame pagalbinį lyginį

$$x^{p-1}-1-(x-1)(x-2)\ldots(x-p+1)\equiv 0\,(\mathrm{mod}\,p). \tag{4.28}$$

Akivaizdu, kad tas lyginys turi $p-1$ sprendinį, kuriems atstovauja skaičiai $k=1,\ 2,\ \ldots,\ p-1$. Iš tikrųjų pagal Ferma teoremą

$$k^{p-1}\equiv 1\,(\mathrm{mod}\,p).$$

Vadinasi, (4.28) lyginio kairioji pusė lygsta 0 moduliu p, kai $x=1,\ 2,\ \ldots,\ p-1$.

Tačiau (4.28) lyginio kairiojoje pusėje esančio polinomo laipsnis ne didesnis už p. Pagal 65 teoremą visi to polinomo koeficientai dalijasi iš p. Laisvasis narys lygus

$$-1-(-1)^{p-1}1\cdot 2\ldots(p-1)=-\big(1+(p-1)!\big).$$

Iš čia ir išplaukia teoremos tvirtinimas.

67 teorema. *Jeigu* n *yra sudėtinis skaičius, tai*

$$(n-1)!+1\not\equiv 0\,(\mathrm{mod}\,n).$$

Įrodymas. Jeigu $n=ab$, tai abu tie netrivialūs dalikliai mažesni už n ir todėl dalija $(n-1)!$. Iš lyginio

$$(ab-1)!+1\equiv 0\,(\mathrm{mod}\,ab)$$

gauname

$$(ab-1)!+1\equiv 0 \pmod{a}.$$

Iš čia

$$1\equiv 0 \pmod{a},$$

o tai yra neteisinga.

Išvada. *Būtina ir pakankama sąlyga, kad sveikasis skaičius* $n>1$ *būtų pirminis, yra*

$$(n-2)!\equiv 1 \pmod{n}. \tag{4.29}$$

Įrodymas.

$$(n-1)!+1=(n-2)!\,(n-1)+1=n\,(n-2)!-(n-2)!+1\equiv$$

$$\equiv -(n-2)!+1 \pmod{n}.$$

Jeigu n yra pirminis skaičius, tai pagal Vilsono teoremą

$$(n-1)!+1\equiv 0 \pmod{n}.$$

Iš čia išplaukia (4.29) lyginys.

Įrodėme sąlygos būtinumą. Jos pakankamumas akivaizdus: jeigu (4.29) teiginys teisingas, tai $(n-1)!+1\equiv 0 \pmod{n}$. Vadinasi, n negali būti sudėtinis.

Ši išvada taip pat žinoma *Leibnico teoremos* pavadinimu.

Pavyzdžiui, pirminis skaičius $p=7$ dalija skaičių $721=6!+1$. Kai $n=6$, tada $(n-1)!+1=121$ ir $6\nmid 121$.

Uždaviniai

13. Išspręskite lyginius:

1) $11x^{10}+5x^5-12x+6\equiv 0 \pmod{5}$;
2) $4x^5+x^3+9x^2+x-2\equiv 0 \pmod{3}$;
3) $9x^7+3x^3+10x+3\equiv 0 \pmod{5}$.

§39. Kvadratiniai lyginiai

Bendruoju atveju antrojo laipsnio, arba kvadratiniai, lyginiai su vienu kintamuoju užrašomi šitaip:

$$Ay^2+By+C\equiv 0 \pmod{m}.$$

Žinodami modulio m kanoninį skaidinį, pagal 61 teoremą tą lyginį galime pakeisti lyginių moduliais p^α sistema. 37 paragrafe matėme, kad pastarųjų lyginių sprendimas pakeičiamas lyginių pirminiais moduliais p sprendimu. Todėl nagrinėsime tik lyginius

$$by^2+cy+d\equiv 0 \pmod{p}. \tag{4.30}$$

Tarkime, kad $(p, b)=1$. Priešingu atveju turėtume pirmojo laipsnio lyginį, kurio sprendimą jau išnagrinėjome. Taip pat apsiribosime atveju, kai $p>2$.

Lyginiai moduliu 2 sprendžiami paprastai: tikrinamos 2 liekanų klasės moduliu 2, jų atstovais galima imti 0 ir 1.

(4.30) *pavidalo lyginį galima pakeisti ekvivalenčiu paprastesnio pavidalo lyginiu*

$$x^2 \equiv a \pmod{p}. \tag{4.31}$$

Įrodymas. Tarkime, kad lyginyje

$$by^2 + cy + d \equiv 0 \pmod{p}$$

koeficientas c yra lyginis. Jeigu c – nelyginis, jį visuomet galima pakeisti lyginiu koeficientu pridėjus modulio kartotinį py. Pažymėję $c = 2f$, gauname

$$b^2 y^2 + 2fby + db \equiv 0 \pmod{p},$$

arba

$$(by + f)^2 \equiv -db - f^2 \pmod{p}.$$

Pažymėję

$$x \equiv by + f \pmod{p},$$

$$-db - f^2 = a,$$

gauname (4.31) pavidalo lyginį. Kadangi $(b, p) = 1$, tai iš pastarojo lyginio galime rasti y, jei žinome x, ir atvirkščiai. Taigi užtenka mokėti spręsti

$$x^2 \equiv a \pmod{p}$$

pavidalo kvadratinius lyginius.

Pavyzdys. Pertvarkysime lyginį

$$17y^2 - 12y + 15 \equiv 0 \pmod{31}.$$

Sudarome pilnąjį kvadratą

$$(17y - 6)^2 - 36 + 15 \equiv 0 \pmod{31}.$$

Tarkime, kad

$$x \equiv 17y - 6 \pmod{31}.$$

Tada kvadratinį lyginį galime užrašyti šitaip:

$$x^2 \equiv 21 \pmod{31}.$$

68 teorema. *Jeigu* $(a, p) = 1$, $p > 2$, *tai lyginys*

$$x^2 \equiv a \pmod{p}$$

turi arba du sprendinius, kurie yra viena kitai priešingos klasės, arba nė vieno.

Įrodymas. Pagal 64 teoremą to lyginio sprendinių skaičius ne didesnis už 2. Jeigu x_0 tenkina lyginį, tai ir $-x_0$ tenkina tą patį lyginį. Tie skaičiai atstovauja skirtingoms klasėms, nes lyginys

$$x \equiv -x_0 \pmod{p}$$

reiškia, kad

$$2x_0 \equiv 0 \pmod{p}, \quad \text{arba} \quad p \mid 2x_0.$$

Kadangi $p \nmid 2$, tai $p \mid x_0$. Tačiau iš

$$x_0 \equiv 0 \pmod{p}$$

gauname

$$a \equiv x_0^2 \equiv 0 \pmod{p}.$$

Tai prieštarauja teoremos prielaidai, kad $(a, p)=1$.

Teorema įrodyta.

Jeigu $(a, p)=1$ *ir lyginys*

$$x^2 \equiv a \pmod{p}$$

yra išsprendžiamas, tai a vadinamas kvadratine liekana moduliu p.

Visas liekanų klases pirminiu moduliu p, išskyrus nulinę klasę, galima suskirstyti į 2 grupes: vienai grupei priklauso liekanų klasės, sudarytos iš kvadratinių liekanų moduliu p, kitai – skaičiai, kurie nėra kvadratinės liekanos tuo moduliu (*kvadratinės neliekanos*).

Iš tikrųjų, jeigu $a \equiv b \pmod{p}$, tai lyginiai

$$x^2 \equiv a \pmod{p},$$

$$x^2 \equiv b \pmod{p}$$

kartu išsprendžiami arba neišsprendžiami.

Pavyzdys. Moduliu 7 turime 6 liekanų klases, tarpusavyje pirmines su moduliu:

$$K_1, K_2, K_3, K_4, K_5, K_6.$$

Lyginiai

$$x^2 \equiv 1 \pmod{7},$$

$$x^2 \equiv 2 \pmod{7},$$

$$x^2 \equiv 4 \pmod{7}$$

išsprendžiami. Jų sprendiniai atitinkamai yra liekanų klasės (abu kvadratinio lyginio sprendiniai rašomi kartu)

$$x \equiv \pm 1 \pmod{7},$$

$$x \equiv \pm 3 \pmod{7},$$

$$x \equiv \pm 2 \pmod{7}.$$

Kiti 3 lyginiai

$$x^2 \equiv 3 \pmod{7},$$

$$x^2 \equiv 5 \pmod{7},$$

$$x^2 \equiv 6 \pmod{7}$$

sprendinių neturi. Tuo galima įsitikinti patikrinus visų liekanų klasių moduliu 7 atstovus kiekvienam tų lyginių.

Liekanų klasės

$$K_1,\ K_2,\ K_4,$$

kurioms priklauso kvadratinės liekanos 1, 2, 4, yra kvadratinių liekanų klasės. Kitos 3 klasės

$$K_3,\ K_5,\ K_6$$

nėra kvadratinių liekanų klasės moduliu 7.

Uždaviniai

14. Užrašykite dvinariu pavidalu šiuos lyginius:

1) $10x^2-x+7\equiv 0 \pmod{13}$;
2) $11x^2+12x+13\equiv 0 \pmod{17}$;
3) $2x^2+x-40\equiv 0 \pmod{19}$;
4) $40x^2+60x+1\equiv 0 \pmod{23}$.

15. Nustatykite, kurios liekanų moduliu m klasės yra kvadratinių liekanų klasės, kai:

1) $m=5$; 2) $m=11$; 3) $m=13$; 4) $m=17$.

16. Parašykite po 10 kvadratinių liekanų moduliu m, kai:

1) $m=11$; 2) $m=13$; 3) $m=23$; 4) $m=29$.

17. Parašykite po 10 kvadratinių liekanų moduliu m, kai:

1) $m=17$; 2) $m=31$; 3) $m=37$; 4) $m=41$.

§40. Oilerio ir Gauso kriterijai

Oilerio kriterijus kvadratinėms liekanoms. Iš praeito paragrafo pavyzdžio matome, kad iš redukuotųjų liekanų klasių moduliu 7 yra 3 kvadratinių liekanų ir 3 kvadratinių neliekanų klasės. Visų redukuotųjų liekanų klasių pasidalijimas pusiau į kvadratinių liekanų ir neliekanų klases nėra atsitiktinis.

69 teorema. *Redukuotoje liekanų sistemoje moduliu p yra* $\frac{p-1}{2}$, $p>2$, *kvadratinių liekanų ir tiek pat kvadratinių neliekanų.*

Įrodymas. Kvadratinės liekanos moduliu p lygsta tuo pačiu moduliu sveikojo skaičiaus pilnajam kvadratui ir atvirkščiai, jeigu a lygsta b^2 moduliu p, tai b yra lyginio

$$x^2\equiv a \pmod{p}$$

sprendinys. Taigi a yra kvadratinė liekana moduliu p.

Vadinasi, kiekvienoje kvadratinių liekanų klasėje turi būti kvadratas. Todėl užtenka nagrinėti kvadratus

$$1^2,\ 2^2,\ 3^2,\ \ldots,\ (p-1)^2. \tag{4.32}$$

Kitų skaičių, tarpusavyje pirminių su p, kvadratai lygsta vienam iš tų kvadratų.

(4.32) sekoje vienodai nuo abiejų galų nutolę kvadratai priklauso toms pačioms liekanų klasėms. Iš tikrųjų nesunku įsitikinti, kad

$$k^2\equiv (p-k)^2 \pmod{p}.$$

Pakanka (4.32) sekoje palikti tik pusę visų kvadratų:

$$1^2,\ 2^2,\ 3^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2. \tag{4.33}$$

Tie kvadratai atstovauja skirtingoms kvadratinių liekanų klasėms. Iš tikrųjų, tarę, kad

$$k^2 \equiv l^2 \pmod p,$$

kai

$$1 \leqslant k < l \leqslant \frac{p-1}{2},$$

gautume

$$(l-k)(l+k) \equiv 0 \pmod p.$$

Tačiau tas lyginys nėra galimas, nes abu daugikliai kairiojoje pusėje teigiami ir mažesni už p, todėl jie negali dalytis iš p, kai $l \neq k$.

Nustatėme, kad visų skaičių, tarpusavyje pirminių su moduliu p, kvadratai patenka į $\frac{p-1}{2}$ skirtingų liekanų klasių, kurių atstovai yra (4.33) skaičiai. Kitos tarpusavyje pirminės su moduliu p klasės nėra kvadratinių liekanų moduliu p klasės, jų yra tiek pat, kiek yra liekanų klasių moduliu p.

70 teorema. (Oilerio kriterijus). *Jeigu* $(a, p)=1$, $p>2$, *tai*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p, & \textit{kai } a-\textit{kvadratinė liekana} \bmod p, \\ -1 \pmod p, & \textit{kai } a-\textit{kvadratinė neliekana} \bmod p. \end{cases}$$

Įrodymas. Remdamiesi Ferma teorema, gauname

$$a^{p-1} - 1 \equiv 0 \pmod p,$$

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Vadinasi, arba

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p, \tag{4.34}$$

arba

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{4.35}$$

Abu tie lyginiai kartu negali būti teisingi, nes tokiu atveju juos sudėję gautume $p \mid a$.

Tarkime, kad lyginys $x^2 \equiv a \pmod p$ išsprendžiamas, t. y. egzistuoja toks sveikasis skaičius x_0, kad

$$x_0^2 \equiv a \pmod p;$$

čia $(x_0, p)=1$. Priešingu atveju vėl gautume, kad $p \mid a$. Abi lyginio puses pakelsime $\frac{p-1}{2}$ laipsniu:

$$x_0^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Pagal Ferma teoremą tuo atveju teisingas (4.34) lyginys. Kadangi yra $(p-1)/2$ skaičių iš skirtingų liekanų klasių moduliu p ir jie tenkina lyginį $x^2 \equiv a \pmod{p}$, tai tiek yra ir lyginio

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

sprendinių. Tačiau iš 64 teoremos išplaukia, kad daugiau jų ir negali būti. Taigi kitos a reikšmės tenkina (4.35) lyginį.

Pavyzdys. Nustatysime, ar lyginys

$$x^9 \equiv 3 \pmod{19}$$

yra išsprendžiamas. Pagal Oilerio kriterijų reikia skaičiuoti 3^9. Taigi

$$3^3 \equiv 27 \equiv 8 \pmod{19},$$

$$3^6 \equiv 64 \equiv 7 \pmod{19},$$

$$3^9 \equiv 56 \equiv -1 \pmod{19}.$$

Lyginys sprendinių neturi.

Gauso kriterijus kvadratinėms liekanoms.

71 teorema. *Tarkime, kad* $(a, p)=1$, $p>2$. *Jeigu visas sandaugas*

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a \tag{4.36}$$

pakeisime absoliučiai mažiausiomis liekanomis moduliu p, tarp kurių bus μ *neigiamų, tai gausime*

$$a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p}. \tag{4.37}$$

Įrodymas. Absoliučiai mažiausių liekanų sistema moduliu p yra

$$-\frac{p-1}{2},\ -\frac{p-1}{2}+1,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{p-1}{2}-1,\ \frac{p-1}{2}. \tag{4.38}$$

Visi (4.38) sekos skaičiai priklauso skirtingoms liekanų klasėms. Kaip jau žinome (50 teorema), redukuotųjų liekanų sistemą 1, 2, ..., $p-1$ padaugine iš tarpusavyje pirminio su p skaičiaus a, gausime skaičius, kurie nelygsta

vienas kitam moduliu p. Todėl galime užrašyti lyginius tarp tose pačiose liekanų klasėse esančių skaičių, nurodytų (4.36) ir (4.38) sekose:

$$\begin{cases} a \equiv \pm r_1 \equiv \varepsilon_1 r_1 \pmod p, \\ 2a \equiv \pm r_2 \equiv \varepsilon_2 r_2 \pmod p, \\ \cdots\cdots\cdots\cdots\cdots \\ \dfrac{p-1}{2}\, a \equiv r_{\frac{p-1}{2}} \equiv \varepsilon_{\frac{p-1}{2}}\, r_{\frac{p-1}{2}} \pmod p. \end{cases}$$

Skaičiai $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ priklauso aibei $\left\{ 1, 2, \ldots, \dfrac{p-1}{2} \right\}$, $\varepsilon_1 = \pm 1$.

Įrodysime, kad $r_k \neq r_j$, jei $k \neq j$. Iš tikrųjų iš lygybės

$$r_k = r_j$$

išplauktų

$$ka \equiv \varepsilon_k r_k \pmod p,$$

$$ja \equiv \varepsilon_j r_k \pmod p.$$

Priklausomai nuo ε_k, ε_j ženklų, sudėję ar atėmę tuos lyginius, dešiniojoje pusėje gautume 0 ir

$$a(k \pm j) \equiv 0 \pmod p.$$

Tačiau tas lyginys negalimas: nei a, nei $k \pm j$ nesidalija iš p, nes jie absoliutiniu didumu mažesni už p. Iš to išplaukia, kad

$$\left\{ r_1, r_2, \ldots, r_{\frac{p-1}{2}} \right\} = \left\{ 1, 2, \ldots, \frac{p-1}{2} \right\}.$$

Panariui sudauginę visus (4.39) sistemos lyginius, gauname

$$a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \ldots \frac{p-1}{2} = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\frac{p-1}{2}}\, r_1 r_2 \ldots r_{\frac{p-1}{2}} \pmod p.$$

Iš čia išplaukia (4.37) lyginys.

Pavyzdys. Remdamiesi Gauso kriterijumi, išspręsime ankstesniame paragrafe nagrinėtą uždavinį ($a=3$, $p=19$). Sudarome (4.36) pavidalo sandaugas:

$$3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27.$$

Pakeitę jas absoliučiai mažiausiomis liekanomis moduliu 19, gauname

$$3,\ 6,\ 9,\ -7,\ -4,\ -1,\ 2,\ 5,\ 8.$$

Matome, kad $\mu=3$. Vadinasi,

$$3^{\frac{p-1}{2}} = 3^9 \equiv (-1)^8 \equiv -1 \pmod{19}.$$

Taigi 3 yra kvadratinė neliekana moduliu 19.

18. Naudodamiesi Oilerio kriterijumi, nustatykite, kurie iš skaičių 41, 43, 44, 45, 46, 47 yra kvadratinės liekanos moduliu 7.

19. Remdamiesi Oilerio kriterijumi, nustatykite, ar išsprendžiami šie lyginiai:

1) $x^2 \equiv 3 \pmod{13}$;
2) $x^2 \equiv 7 \pmod{17}$;
3) $x^2 \equiv 2 \pmod{19}$;
4) $x^2 \equiv -11 \pmod{23}$;
5) $x^2 \equiv 4 \pmod{29}$.

20. Naudodamiesi Gauso kriterijumi, nustatykite, kurie iš skaičių 31, 32, 33, 34, 36, 37 nėra kvadratinės liekanos moduliu 7.

21. Naudodamiesi Gauso kriterijumi, nustatykite, kurie iš skaičių, nurodytų 18 uždavinyje, nėra kvadratinės liekanos moduliu 7.

22. Remdamiesi Gauso kriterijumi, nustatykite, kurie iš šių lyginių išsprendžiami:

1) $x^2 \equiv 2 \pmod{11}$;
2) $x^2 \equiv -3 \pmod{13}$;
3) $x^2 \equiv 5 \pmod{17}$;
4) $x^2 \equiv 19 \pmod{23}$;
5) $x^2 \equiv -10 \pmod{31}$.

23. Naudodamiesi Gauso kriterijumi, nustatykite, kurie iš 19 uždavinyje nurodytų lyginių yra išsprendžiami.

§41. Ležandro simbolis

Kvadratinių lyginių teorijoje svarbią vietą užima *Ležandro* (A. Legendre, 1752–1833, prancūzų matematikas) įvestas simbolis, vadinamas jo vardu. Ležandro simbolis vartojamas ne tik lyginių teorijoje, bet ir algebroje bei skaičių teorijoje.

Ležandro simbolį $\left(\frac{a}{p}\right)$, p – nelyginis pirminis skaičius, $(a, p)=1$, apibrėžiame šitaip:

$$\left(\frac{a}{p}\right)=\begin{cases} 1, & \text{kai } a-\text{kvadratinė liekana mod}\, p, \\ -1, & \text{kai } a-\text{kvadratinė neliekana mod}\, p. \end{cases}$$

Iš apibrėžimo išplaukia šitokios to simbolio savybės:

1) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$,

2) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$,

3) $\left(\frac{a_1 a_2 \ldots a_k}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\ldots\left(\frac{a_k}{p}\right)$,

4) $\left(\frac{a^2 b}{p}\right)=\left(\frac{b}{p}\right)$,

5) $\left(\frac{1}{p}\right)=1$,

6) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$,

7) $\left(\frac{a}{p}\right)=(-1)^{\mu}$;

čia μ – skaičius, apibrėžtas 71 teoremoje.

Pirmoji savybė akivaizdi. Minėjome, kad skaičiai, kurie lygsta moduliu p, arba visi yra, arba visi nėra kvadratinės liekanos moduliu p.

Antroji savybė išplaukia iš Oilerio kriterijaus.

Įrodysime trečiąją savybę:

$$\left(\frac{a_1 a_2 \ldots a_k}{p}\right)\equiv(a_1 a_2 \ldots a_k)^{\frac{p-1}{2}}\equiv a_1^{\frac{p-1}{2}} a_2^{\frac{p-1}{2}} \ldots a_k^{\frac{p-1}{2}}\equiv$$

$$\equiv\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\ldots\left(\frac{a_k}{p}\right)\pmod p.$$

Abi to lyginio pusės yra skaičiai, lygūs ± 1. Jų skirtumo absoliutinis didumas ne didesnis už 2, todėl iš p gali dalytis tik tuo atveju, kai tas skirtumas lygus 0. Taigi abi lyginio pusės yra lygios.

Iš trečiosios savybės lengvai išplaukia ketvirtoji:

$$\left(\frac{a^2 b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{b}{p}\right).$$

Penktoji savybė teisinga todėl, kad lyginys

$$x^2\equiv 1\pmod p$$

visuomet išsprendžiamas. Jo sprendiniai yra

$$x\equiv\pm 1\pmod p.$$

Šeštoji savybė išplaukia iš antrosios:

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\pmod p.$$

Panašiai kaip ir trečiosios savybės įrodyme, įsitikiname, kad tas lyginys iš tikrųjų yra lygybė.

Paskutinė savybė išplaukia iš Gauso kriterijaus kvadratinėms liekanoms.

Pavyzdys. Naudodamiesi Ležandro simboliu, nustatysime, ar išsprendžiamas lyginys

$$x^2\equiv 15\pmod{17}.$$

Skaičiuosime Ležandro simbolį

$$\left(\frac{15}{17}\right).$$

Kadangi

$$\left(\frac{15}{17}\right)=\left(\frac{15+17}{17}\right)=\left(\frac{32}{17}\right)=\left(\frac{2\cdot 4^2}{17}\right)=\left(\frac{2}{12}\right)=\left(\frac{2+2\cdot 17}{17}\right)=\left(\frac{36}{17}\right)=\left(\frac{6}{17}\right)^2=1,$$

tai lyginys išsprendžiamas.

Toks Ležandro simbolio skaičiavimo būdas kartais gali būti gana ilgas. Skaičiavimai sutrumpėja pasinaudojus dar viena Ležandro simbolio savybe, kuri vadinama *Ležandro simbolio apvertimo dėsniu.*

Visi Ležandro simbolio apvertimo dėsnio įrodymai gana sudėtingi, čia jų nenagrinėsime (vadovėlio I leidime buvo pateiktas Gauso sukurtas įrodymas).

Ležandro simbolio apvertimo dėsnis. *Jeigu p ir q yra skirtingi nelyginiai pirminiai skaičiai, tai*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Jeigu $p>2$ – pirminis skaičius, tai

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Naudodamiesi Oilerio ir Gauso kriterijais, taip pat Ležandro simboliu, galime nustatyti, ar lyginys

$$x^2\equiv a\,(\mathrm{mod}\,p)$$

išsprendžiamas, kai p – pirminis skaičius, $(a, p)=1$.

Jeigu lyginys išsprendžiamas, tai jo sprendinius galima rasti tikrinant visas liekanų klases. Galima taip pat mėginti rasti tokį skaičių b, su kurio kvadratu lygtų a moduliu p:

$$a\equiv b^2\,(\mathrm{mod}\,p).$$

Tuo atveju dviem sprendiniams atstovautų skaičiai b ir $-b$.

Pavyzdžiui, prie lyginio $x^2\equiv 23$ (mod 11) dešiniosios pusės pridėję modulio kartotinį 77, gauname lyginį $x^2\equiv 10^2$ (mod 11), kurio sprendiniai yra liekanų klasės K_{10} ir $K_{-10}=K_1$.

Paprastai Ležandro simbolio apvertimo dėsnį užrašome šitaip:

$$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Pavyzdžiai. 1. Nustatysime, ar išsprendžiamas lyginys

$$x^2\equiv 82\,(\mathrm{mod}\,113).$$

Skaičiuojame Ležandro simbolį, remdamiesi anksčiau nurodytomis jo savybėmis bei apvertimo dėsniu:

$$\left(\frac{82}{113}\right)=\left(\frac{2\cdot 41}{113}\right)=\left(\frac{2}{113}\right)\left(\frac{41}{113}\right)=(-1)^{\frac{113^2-1}{8}}\left(\frac{41}{113}\right)=\left(\frac{41}{113}\right)=$$

$$=(-1)^{\frac{113-1}{2}\cdot\frac{41-1}{2}}\left(\frac{113}{41}\right)=\left(\frac{113}{41}\right)=\left(\frac{31}{41}\right)=(-1)^{\frac{31-1}{2}\cdot\frac{41-1}{2}}\left(\frac{41}{31}\right)=$$

$$=\left(\frac{41}{31}\right)=\left(\frac{10}{31}\right)=\left(\frac{2}{31}\right)\left(\frac{5}{31}\right)=(-1)^{\frac{31^2-1}{8}}\left(\frac{5}{31}\right)=\left(\frac{5}{31}\right)=$$

$$=(-1)^{\frac{5-1}{2}\cdot\frac{31-1}{2}}\left(\frac{31}{5}\right)=\left(\frac{31}{5}\right)=\left(\frac{1}{5}\right)=1.$$

Lyginys yra išsprendžiamas.

2. Skaičiuosime Ležandro simbolį $\left(\frac{57}{211}\right)$:

$$\left(\frac{57}{211}\right)=\left(\frac{3}{211}\right)\left(\frac{19}{211}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{211-1}{2}}\left(\frac{211}{3}\right)(-1)^{\frac{19-1}{2}\cdot\frac{211-1}{2}}\left(\frac{211}{19}\right)=$$

$$=\left(\frac{211}{3}\right)\left(\frac{211}{19}\right)=\left(\frac{1}{3}\right)\left(\frac{2}{19}\right)=\left(\frac{2}{19}\right)=(-1)^{\frac{19^2-1}{8}}=-1.$$

Kadangi $\left(\frac{57}{211}\right)=-1$, tai kvadratinis lyginys

$$x^2\equiv 57 \pmod{211}$$

neišsprendžiamas.

Ležandro simboliai taikomi nagrinėjant ir kitas matematikos problemas. 29 teoremoje buvo įrodyta, kad yra be galo daug $-1+4t$ bei $-1+6t$ pavidalo pirminių skaičių. Naudodamiesi Ležandro simboliu, įrodysime šitokią teoremą.

72 teorema. *Egzistuoja be galo daug* $1+4t$ *bei* $1+6t$ *pavidalo pirminių skaičių.*

Įrodymas. Tarkime priešingai, $1+4t$ pavidalo pirminių skaičių aibė yra baigtinė. Pažymėkime tų pirminių skaičių sandaugą N ir tarkime, kad p yra pirminis skaičiaus $4N^2+1$ daliklis. Tai reiškia, kad

$$(2N)^2\equiv -1 \pmod{p}.$$

Taigi -1 yra kvadratinė liekana moduliu p. Vadinasi, Ležandro simbolis lygus 1:

$$\left(\frac{-1}{p}\right)=1.$$

Tačiau iš 6 Ležandro simbolio savybės išplaukia, kad

$$(-1)^{\frac{p-1}{2}}=1.$$

Ši lygybė galima tik tada, kai $p-1$ yra 4 kartotinis, taigi $p=1+4t$. Tokio pavidalo pirminių skaičių sandauga buvo pažymėta N, todėl $p \mid N$. Tačiau pirminis skaičius p, kaip skaičių $4N^2+1$ ir N daliklis, turi dalyti ir 1. Gavome prieštaravimą. Taigi prielaida, kad $1+4t$ pavidalo pirminių skaičių aibė baigtinė, yra neteisinga.

Dabar įrodysime, kad yra be galo daug $1+6t$ pavidalo pirminių skaičių.

Tarkime, kad $6t+1$ pavidalo pirminių skaičių yra tik baigtinis skaičius. Jų sandaugą žymėkime N. Pradžioje išsiaiškinsime, kokioms liekanų klasėms moduliu 12 priklauso pirminiai skaičiai. Skaičiai 1, 5, 7, 11 atstovauja klasėms, tarpusavyje pirminėms su 12. Vadinasi,

$$p=12k+r,\ r=1,\ 5,\ 7,\ 11.$$

Skaičiuosime Ležandro simbolį $\left(\frac{-3}{p}\right)$ remdamiesi apvertimo dėsniu bei kitomis Ležandro simbolio savybėmis:

$$\left(\frac{-3}{p}\right)=\left(\frac{-3}{12k+r}\right)=\left(\frac{-1}{12k+r}\right)\left(\frac{3}{12k+r}\right)=(-1)^{\frac{12k+r-1}{2}}\left(\frac{3}{12k+r}\right)=$$

$$=(-1)^{\frac{r-1}{2}}\left(\frac{12k+r}{3}\right)(-1)^{\frac{12k+r-1}{2}\cdot\frac{3-1}{2}}=(-1)^{r-1}\left(\frac{r}{3}\right)=\left(\frac{r}{3}\right).$$

Nesunku įsitikinti, kad Ležandro simbolis $\left(\frac{r}{3}\right)=1$, kai $r=1$ ir $r=7$ (tai atitinka atvejį, kai $p\equiv 1 \pmod 6$). Kitais dviem atvejais $r=5$ ir $r=11$ (tai atitinka atvejį, kai $p\equiv 5 \pmod 6$), $\left(\frac{r}{3}\right)=-1$. Vadinasi,

$$\left(\frac{-3}{p}\right)=1 \Leftrightarrow p\equiv 1 \pmod 6.$$

Tolesnė įrodymo eiga panaši į pirmosios teoremos dalies įrodymą.

Raide p pažymėsime bet kurį pirminį skaičiaus $4N^2+3$ daliklį. Taigi teisingas lyginys

$$(2N)^2\equiv -3 \pmod p.$$

Vadinasi, -3 yra kvadratinė liekana moduliu p ir $p\equiv 1 \pmod 6$. Iš čia $p \mid N$. Iš šio dalumo sąryšio bei iš $p \mid (4N^2+3)$ išplaukia, kad $p \mid 3$. Taigi $p=3$. Bet tai prieštarauja įrodytam teiginiui, jog tokie p pasižymi savybe $p\equiv 1 \pmod 6$.

Teorema įrodyta.

Taikant Ležandro simbolį ir lyginių savybes, galima nustatyti kai kurių Diofanto lygčių neišsprendžiamumą.

Pavyzdžiai. 1. Tirsime Diofanto lygtį

$$3x^2+7y^3=11.$$

Pereidami nuo lygybės prie lyginio moduliu 7, gauname

$$3x^2\equiv 11 \pmod 7,$$

$$3x^2\equiv 11+7 \pmod 7,$$

$$x^2\equiv 6 \pmod 7.$$

Jeigu Diofanto lygtis $3x^2+7y^3=11$ yra išsprendžiama, tai turi būti išsprendžiamas ir užrašytasis lyginys. Naudodamiesi Ležandro simboliu, nustatysime, ar tas lyginys išsprendžiamas:

$$\left(\frac{6}{7}\right)=\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)=(-1)^{\frac{49-1}{8}}\left(\frac{3}{7}\right)=\left(\frac{3}{7}\right)=\left(\frac{7}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}=$$

$$=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1.$$

Kadangi Ležandro simbolio reikšmė lygi -1, tai kvadratinis lyginys, kartu ir Diofanto lygtis neturi sprendinių.

2. Nagrinėkime Diofanto lygtį

$$26x^2+5x+125=12.$$

Pakeitę šią lygtį lyginiu moduliu 5, gauname

$$x^2\equiv 2 \pmod 5.$$

Ir šis lyginys neturi sprendinių, nes $\left(\frac{2}{5}\right)=-1$.

Uždaviniai

24. Remdamiesi Ležandro simboliu ir Gauso kriterijumi, nustatykite, ar šie lyginiai išsprendžiami:

1) $x^2-x-1\equiv 0 \pmod 7$; 2) $x^2\equiv 11 \pmod{13}$; 3) $x^2\equiv 8 \pmod{17}$; 4) $x^2\equiv 21 \pmod{37}$.

25. Raskite visas kvadratinių liekanų klases moduliais 11, 13, 17.

26. Apskaičiuokite Ležandro simbolius:

$$\left(\frac{45}{89}\right),\ \left(\frac{-11}{89}\right),\ \left(\frac{37}{89}\right),\ \left(\frac{1000}{89}\right),\ \left(\frac{41317}{89}\right),\ \left(\frac{13}{117}\right),\ \left(\frac{26}{117}\right),$$

$$\left(\frac{39}{117}\right),\ \left(\frac{81}{117}\right),\ \left(\frac{49}{117}\right),\ \left(\frac{129}{117}\right),\ \left(\frac{91}{181}\right),\ \left(\frac{101}{181}\right),\ \left(\frac{122}{181}\right),\ \left(\frac{99}{181}\right),$$

$$\left(\frac{272}{181}\right),\ \left(\frac{378}{181}\right),\ \left(\frac{999}{181}\right),\ \left(\frac{101}{181}\right),\ \left(\frac{10^{35}}{181}\right).$$

27. Naudodamiesi Ležandro simboliu, įrodykite, kad Diofanto lygtys

$$x^2+47y^2=73,\quad 132x^2+63y^2=131$$

neišsprendžiamos.

28. Įrodykite, kad dviejų iš eilės einančių sveikųjų skaičių sandauga negali lygti 1 moduliu 13.

29. Įrodykite, kad kvadratinių lygčių diskriminantai negali būti $4n+2$ ar $4n+3$ pavidalo skaičiai.

30. Įrodykite, kad lyginys $x^2\equiv -11 \pmod{4p}$ neišsprendžiamas, jei pirminis skaičius p yra $p=11n+2$ pavidalo.

31. Ar gali pirmųjų n natūrinių skaičių suma baigtis skaitmeniu 7?

32. Raskite tuos pirminius skaičius p, su kuriais 3 yra kvadratinė liekana.

Laipsninės liekanos

§42. Rodiklis moduliu ir jo savybės

Oilerio teorema teigia, kad bet kuriam tarpusavyje pirminiam su moduliu m skaičiui a teisingas sąryšis

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Pasitaiko atvejų, kai natūrinis rodiklis k, su kuriuo teisingas lyginys

$$a^k \equiv 1 \pmod{m}, \tag{5.1}$$

žymiai mažesnis už $\varphi(m)$. Tačiau yra tokių modulių m ir skaičių a, su kuriais (5.1) lyginyje negali būti $k < \varphi(m)$.

Pavyzdžiui, kai $m=10$, tarpusavyje pirminės su moduliu yra 4 liekanų klasės: K_1, K_3, K_7, K_9. Imkime iš tų klasių skaičius 1, 3, 7, 9:

$1^1 \equiv 1 \pmod{10}$,

$3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 7$, $3^4 \equiv 1 \pmod{10}$,

$7^1 \equiv 7$, $7^2 \equiv 9$, $7^3 \equiv 3$, $7^4 \equiv 1 \pmod{10}$,

$9^1 \equiv 9$, $9^2 \equiv 1 \pmod{10}$

Matome, kad mažiausias natūrinis rodiklis k, su kuriuo teisingas lyginys (5.1) nevienodas skirtingiems a. Skaičiui 1 šis k lygus 1, skaičiui $9-k$ lygus 2, kitiems dviem skaičiams 3 ar 7 jis lygus 4. Beje, $\varphi(10)=4$.

Taigi Oilerio teorema teisinga su visais 4 skaičiais, visų jų 4-asis laipsnis lygsta 1 moduliu 10, tačiau skaičiai 1 ir 9 lygsta 1 ir su mažesniu negu 4 rodikliu k.

Šis pavyzdys rodo, kad, imant kiekvieną tarpusavyje pirminį su 10 skaičių, galima rasti atitinkamą natūrinį k, su kuriuo teisingas (5.1) lyginys. Jis teisingas bet kuriuo moduliu.

Tarpusavyje pirminio su m skaičiaus rodikliu moduliu m vadiname tokį mažiausią natūrinį skaičių δ, su kuriuo

$$a^\delta \equiv 1 \pmod{m}.$$

Pavyzdys. Rasime skaičių 5 ir 2 rodiklius moduliu 7. Kadangi

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1 \pmod{7},$$

o

$$5^1 \equiv 5,\ 5^2 \equiv 4,\ 5^3 \equiv 6,\ 5^4 \equiv 2,\ 5^5 \equiv 3,\ 5^6 \equiv 1 \pmod 7,$$

tai skaičiaus 2 rodiklis moduliu 7 lygus 3, o skaičiaus 5 lygus 6.

Skaičiaus a rodiklį δ moduliu m žymėsime

$$r_m(a), \quad \text{arba} \quad r(a)$$

(jeigu aišku, kuriuo moduliu tas rodiklis apibrėžtas).

Tas pats skaičius a skirtingais moduliais gali turėti skirtingus rodiklius.

73 teorema. *Visi tos pačios liekanų klasės moduliu m skaičiai turi tą patį rodiklį moduliu m, t. y.*

$$a \equiv b \pmod m \Rightarrow r(a) = r(b).$$

Įrodymas. Jeigu $r(b) = \delta$, tai

$$a \equiv b \pmod m \Rightarrow a^\delta \equiv b^\delta \pmod m \Rightarrow a^\delta \equiv 1 \pmod m \Rightarrow r(a) \leqslant r(b).$$

Tačiau lyginyje $a \equiv b \pmod m$ skaičiai a ir b yra simetriški lyginio ženklo atžvilgiu, todėl analogiškai

$$r(b) \leqslant r(a).$$

iš tų dviejų sąlygų išplaukia, kad $r(a) = r(b)$.

Teorema įrodyta.

Visų tos pačios liekanų klasės skaičių rodiklį moduliu m vadiname *liekanų klasės rodikliu moduliu m.*

Liekanų klasės rodiklį moduliu m galima interpretuoti grupių teorijos terminais.

Priminsime, kad grupės G elemento g eile vadiname tokį mažiausią natūrinį skaičių δ, su kuriuo

$$g^\delta = e;$$

čia e – multiplikacinės grupės G vienetinis elementas.

Kadangi lyginį $a^\delta \equiv 1 \pmod m$ galime išreikšti lygybe

$$K_a^\delta = K_1,$$

tai liekanų klasės moduliu m, tarpusavyje pirminės su tuo moduliu, rodiklis moduliu m lygus tos liekanų klasės eilei.

Lagranžo teorema teigia, kad grupės elemento eilė yra gupės eilės daliklis. Kadangi redukuotųjų liekanų klasių moduliu m grupės eilės yra $\varphi(m)$ ($\varphi(m)$ žymima Oilerio funkcija), tai

$$\delta \mid \varphi(m).$$

Taigi nustatėme, kad bet kurio tarpusavyje pirminio su m skaičiaus a rodiklis δ moduliu m yra $\varphi(m)$ daliklis. Tą patį rezultatą toliau gausime ir kitu būdu.

74 teorema. *Jeigu* δ *yra skaičiaus* a, $(a, m)=1$, *rodiklis moduliu* m, *tai skaičiai*

$$a^0,\ a^1,\ a^2,\ \ldots,\ a^{\delta-1} \tag{5.2}$$

priklauso skirtingoms liekanų klasėms moduliu m.

Įrodymas. Jeigu $0 \leqslant l < k \leqslant \delta - 1$ ir, priešingai teoremos tvirtinimui,

$$a^k \equiv a^l \pmod{m},$$

tai

$$a^{k-l} \equiv 1 \pmod{m}.$$

Skaičius $k-l$ yra teigiamas ir mažesnis už δ. Tačiau tai prieštarauja sąlygai, kad δ yra skaičiaus a rodiklis moduliu m.

1 išvada. *Jeigu* $\delta=\varphi(m)$, *tai* (5.2) *pavidalo skaičiai sudaro redukuotąją liekanų sistemą moduliu* m.

Iš tikrųjų turime $\varphi(m)$ skaičių, priklausančių skirtingoms liekanų klasėms moduliu m. Kadangi iš sąryšio $(a, m)=1$ išplaukia sąryšis $(a^k, m)=1$, tai (5.2) sekos skaičiai sudaro r. l. s. moduliu m.

2 išvada. *Jeigu multiplikacinėje liekanų klasių moduliu* m *grupėje* G *yra liekanų klasė* K *su rodikliu* $\varphi(m)$ *moduliu* m, *tai grupė* G *yra ciklinė ir ją generuoja klasė* K_a.

75 teorema. *Jeigu* $r_m(a)=\delta$, *tai lyginys*

$$a^k \equiv a^s \pmod{m}$$

teisingas tada ir tik tada, kai

$$k \equiv s \pmod{\delta}.$$

Įrodymas. Pakankamumas. Tarkime, kad $k \equiv s \pmod{m}$ ir $k \geqslant s$. Tuomet $k=s+\delta t$ $(t \in \mathbf{N})$ ir

$$a^k = a^{s+\delta t} = a^s (a^\delta)^t.$$

Kadangi δ yra skaičiaus a rodiklis moduliu m, tai

$$a^\delta \equiv 1 \pmod{m},$$

$$(a^\delta)^t \equiv 1^t \equiv 1 \pmod{m},$$

ir

$$a^k = a^s (a^\delta)^t \equiv a^s \pmod{m}.$$

Būtinumas. Tarkime, kad

$$a^k \equiv a^s \pmod{m}.$$

Jeigu $k \geqslant s$, tai padaliję abi lyginio puses iš a^s (dalyti galima, nes a, taigi ir a^s, yra tarpusavyje pirminis su moduliu), gauname

$$a^{k-s} \equiv 1 \pmod{m}.$$

Skirtumą $k-s$ padalysime iš δ su liekana:

$$k-s = \delta q + r;$$

čia $0 \leqslant r < \delta$, $q \in \mathbf{Z}$. Tuomet

$$a^{k-s} = a^{\delta q + r} = (a^{\delta})^q a^r.$$

Kadangi δ yra skaičiaus a rodiklis moduliu m, tai, kaip ir anksčiau, gauname

$$a^{k-s} \equiv (1)^q a^r \equiv a^r \pmod{m}.$$

Palyginę šį lyginį su lyginiu $a^{k-s} \equiv 1 \pmod{m}$, matome, kad

$$a^r \equiv 1 \pmod{m}.$$

Jeigu r būtų nelygus 0, tai tas lyginys prieštarautų skaičiaus a rodiklio moduliu m apibrėžimui, nes $r < \delta$. Taigi $r = 0$. Tai rodo, kad

$$k-s = \delta q$$

ir

$$k \equiv s \pmod{\delta}.$$

1 išvada. *Jeigu* $r_m(a) = \delta$, *tai lyginys*

$$a^{\gamma} \equiv 1 \pmod{m}$$

teisingas tada ir tik tada, kai

$$\gamma \equiv 0 \pmod{\delta}.$$

Teiginys išplaukia iš teoremos paėmus $k = \gamma$, $s = 0$.

2 išvada. *Jeigu* $r_m(a) = \delta$, *tai*

$$\delta \mid \varphi(m).$$

Remdamiesi Oilerio teorema, 1 išvadoje imame $\gamma = \varphi(m)$ ir gauname reikiamą teiginį.

Nustatėme kai kuriuos skaičių $k > 0$, pasižyminčių savybe

$$a^k \equiv 1 \pmod{m}, \quad (a, m) = 1,$$

dėsningumus.

Visi tokie natūriniai skaičiai yra skaičiaus a rodiklio moduliu m kartotiniai, priklausantys sekai δ, 2δ, 3δ, ...

Skaičiaus a rodikliu moduliu m gali būti ne bet kuris skaičius, o tik $\varphi(m)$ daliklis.

Pavyzdžiui, bet kurio skaičiaus a, $(a, 14) = 1$, rodiklis moduliu 14 gali būti tik vienas iš skaičių 1, 2, 3, 6, nes tik šie skaičiai yra $\varphi(14) = 6$ dalikliai.

Skaičiaus 1 rodiklis bet kuriuo moduliu m lygus 1:

$$1 \equiv 1 \pmod{m}.$$

Bet kuris skaičius $\varphi(m)$ turi mažiausiai du daliklius: 1 ir $\varphi(m)$. Akivaizdu, kad skaičių $a \equiv 1 \pmod{m}$ rodiklis yra 1. $\varphi(m)$ yra didžiausias galimas rodiklis moduliu m (didžiausias galimas $\varphi(m)$ daliklis). Skaičiai su tuo rodikliu pasižymi keletu svarbių savybių.

§43. Primityviosios šaknys moduliu m

Skaičius a, tarpusavyje pirminis su m, vadinamas primityviąja šaknimi moduliu m, jei

$$r_m(a) = \varphi(m).$$

Liekanų klasė moduliu m, kurios skaičiai yra primityviosios šaknys moduliu m, vadinama primityviąja klase moduliu m.

Primityviosios šaknys iš kitų skaičių, tarpusavyje pirminių su moduliu m, išsiskiria tuo, kad jų rodiklis tuo moduliu yra maksimalus, t. y. lygus $\varphi(m)$.

Dvi primityviosios šaknys moduliu m yra skirtingos, jeigu jos priklauso skirtingoms liekanų klasėms moduliu m.

Pavyzdys. Rasime visų skaičių, tarpusavyje pirminių su 14, rodiklius. Ankstesniame paragrafe matėme, kad tie rodikliai gali būti tik sekos 1, 2, 3, 6 nariai. Turime:

$$\begin{gathered}
3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv -1, \quad 3^6 \equiv 1, \\
5^1 \equiv 5, \quad 5^2 \equiv 11, \quad 5^3 \equiv -1, \quad 5^6 \equiv 1, \\
9^1 \equiv 9, \quad 9^2 \equiv -3, \quad 9^3 \equiv 1, \\
11^1 \equiv 11, \quad 11^2 \equiv 9, \quad 11^3 \equiv 1, \\
13^1 \equiv 13, \quad 13^2 \equiv 1 \pmod{14}.
\end{gathered}$$

Taigi $r(1)=1$, $r(13)=2$, $r(9)=r(11)=3$, $r(3)=r(5)=6$.

Didžiausią galimą rodiklį moduliu 14 turi skaičiai 3 ir 5. Jie ir yra primityviosios šaknys moduliu 14.

Nagrinėdami vieneto šaknis (I dalis, § 44), t. y. lygties

$$x^n = 1$$

sprendinius, įsitikinome, kad yra tokių n-ojo laipsnio vieneto šaknų, kurias keldami laipsniais 0, 1, ..., $n-1$, gauname visas to laipsnio vieneto šaknis. Tokias vieneto šaknis pavadinome *primityviosiomis*. Primityviosios n-ojo laipsnio vieneto šaknys nesutampa su mažesnio laipsnio vieneto šaknimis.

Nesunku įrodyti, kad primityviosios vieneto šaknys ir primityviosios šaknys moduliu m turi panašių savybių.

Liekanų klasė K_a moduliu m yra primityvioji klasė moduliu m, kai ji yra lygties

$$x^n = K_1$$

sprendinys; čia K_1 – vienetinė klasė, $n=\varphi(m)$. Ji nėra žemesnio laipsnio analogiškos lygties sprendinys. Galima įrodyti, kad šią liekanų klasę keldami laipsniais 0, 1, ..., $\varphi(m)-1$, gausime visas liekanų klases, tarpusavyje pirmines su moduliu m. Iš tikrųjų, keldami liekanų klasę K_a nurodytais laipsniais, gausime $\varphi(m)$ liekanų klasių, kurių numeriai bus

$$a^0,\ a^1,\ \ldots,\ a^{\varphi(m)-1}.$$

Tačiau jeigu a yra primityvioji šaknis moduliu m, tai pastarieji skaičiai sudaro r. l. s. moduliu m, jie atstovauja visoms $\varphi(m)$ tarpusavyje pirminių su moduliu m klasių. Taigi liekanų klasių multiplikacinė grupė yra ciklinė grupė (K_a). Taigi turime visišką analogiją su vieneto primityviosiomis šaknimis.

76 teorema. *Jeigu a yra primityvioji šaknis moduliu m, tai a^k $(k>0)$ yra primityvioji šaknis moduliu m tada ir tik tada, kai*

$$\big(k,\ \varphi(m)\big)=1.$$

Įrodymas. Žymėsime $(k,\ \varphi(m))=d$. Jeigu $d>1$, tai $\varphi(m)/d$ ir k/d yra sveikieji teigiami skaičiai, be to,

$$(a^k)^{\varphi(m)/d}=(a^{\varphi(m)})^{k/d}\equiv 1\ (\mathrm{mod}\, m).$$

Vadinasi, kai $d>1$, $r\ (a^k)<\varphi(m)$ ir todėl a^k nėra primityvioji šaknis moduliu m. Įrodėme sąlygos būtinumą.

Tarkime, kad $(k,\ \varphi(m))=1$. Tuomet egzistuoja tokie sveikieji skaičiai u ir v, su kuriais

$$ku+\varphi(m)\,v=1$$

ir

$$(a^\delta)\equiv a^{(ku+\varphi(m)\,v)\delta}\equiv \alpha^{ku\delta}\,(a^{\varphi(m)})^{v\delta}\equiv a^{ku\delta}\ (\mathrm{mod}\, m).$$

Jeigu a^k nėra primityvioji šaknis moduliu m, tai iš to lyginio išplaukia, kad ir a negali būti primityvioji šaknis.

Išvada. *Jeigu moduliu m yra bent viena primityvioji šaknis, tai jų yra $\varphi\big(\varphi(m)\big)$.*

Įrodymas. Iš tikrųjų skaičių k, kurie nelygsta moduliu $\varphi(m)$ ir nėra tarpusavyje pirminiai su moduliu $\varphi(m)$, yra $\varphi\big(\varphi(m)\big)$.

Pavyzdžiui, jeigu yra bent viena primityvioji šaknis moduliu 17, tai iš viso jų yra

$$\varphi\big(\varphi(17)\big)=\varphi(16)=8.$$

Remiantis 76 teorema, kai žinoma viena primityvioji šaknis g, galima rasti visas primityviąsias šaknis moduliu m – reikia g nuosekliai kelti visais tokiais laipsniais k, kad būtų

$$1\leqslant k<\varphi(m),\ \big(k,\ \varphi(m)\big)=1.$$

Pavyzdys. Nustatysime, ar 2 yra primityvioji šaknis moduliu 13. Iš tikrųjų $\varphi(13)=12$. Visi galimi 12 dalikliai yra

$$1,\ 2,\ 3,\ 4,\ 6,\ 12.$$

Užtenka patikrinti tik šiuos 2 laipsnius:

$$2^2\equiv 4,\ 2^3\equiv 8,\ 2^4\equiv 3,\ 2^6\equiv -1,\ 2^{12}\equiv 1 \pmod{13}.$$

Taigi $r(2)=12=\varphi(13)$, 2 yra primityvioji šaknis moduliu 13. Iš viso tuo moduliu yra $\varphi(\varphi(13))=\varphi(12)=4$ primityviosios šaknys. Jas gausime primityviąją šaknį 2 keldami laipsniais, tarpusavyje pirminiais su 12 ir mažesniais už 12, t. y. laipsniais

$$1,\ 5,\ 7,\ 11.$$

Kadangi $2^5\equiv 6,\ 2^7\equiv 11,\ 2^{11}\equiv 10 \pmod{13}$, tai visos 4 primityviosios šaknys moduliu 13 yra

$$2,\ 6,\ 10,\ 11.$$

Jos atstovauja 4 skirtingoms primityviosioms liekanų klasėms moduliu 13.

Įrodysime primityviųjų šaknų egzistavimo kriterijų.

77 teorema. *Jeigu* $\varphi(m)$ *kanoninis skaidinys yra*

$$p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$$

ir jeigu skaičius a, $(a, m)=1$, tenkina sąlygas

$$\begin{aligned} a^{\varphi(m)/p_1} &\not\equiv 1 \pmod{m},\\ a^{\varphi(m)/p_2} &\not\equiv 1 \pmod{m},\\ &\cdots\cdots\cdots\cdots\\ a^{\varphi(m)/p_k} &\not\equiv 1 \pmod{m}, \end{aligned} \tag{5.3}$$

tai a *yra primityvioji šaknis moduliu* m.

Įrodymas. Sąlygų būtinumas akivaizdus. Iš tikrųjų, jeigu bent vienas (5.3) sistemos lyginys yra teisingas, tai

$$r(a)<\varphi(m),$$

ir a nėra primityvioji šaknis.

Jeigu (5.3) sąlygos išpildytos, tai $r(a)$ negali būti netrivialusis $\varphi(m)$ daliklis. Iš tikrųjų, jei būtų $r(a)<\varphi(m)$, tai turėtume

$$\varphi(m)=r(a)\,t,\quad t>1.$$

Jeigu $p_i^l \mid t$, tai p_i yra ir $\varphi(m)$ daliklis. Tačiau tokiu atveju $\dfrac{\varphi(m)}{p_i}=r(a)\dfrac{t}{p_i}$ ir $\dfrac{t}{p_i}$ yra sveikasis skaičius. Tada

$$a^{\varphi(m)/p_i}=(a^{r(a)})^{t/p_i}\equiv 1 \pmod{m},$$

bet tai prieštarauja prielaidai, kad (5.3) sąlygos teisingos.

Teorema įrodyta.

Remiantis 77 teorema, galima sumažinti skaičiavimus tikrinant, ar skaičius yra primityvioji šaknis. Pavyzdžiui, tikrinant, ar a yra primityvioji šaknis moduliu 31, užtenka patikrinti laipsnius

$$a^6,\ a^{10},\ a^{15}.$$

Jeigu bent vienas iš jų lygsta 1 moduliu 31, tai a nėra primityvioji šaknis. Iš tikrųjų

$$\varphi(31)=30=2\cdot 3\cdot 5,$$

$$\frac{\varphi(31)}{2}=15,\quad \frac{\varphi(31)}{3}=10,\quad \frac{\varphi(31)}{5}=6.$$

Taigi tikrinant, ar a yra primityvioji šaknis moduliu 31, pakanka patikrinti, ar teisingi teiginiai

$$a^{15}\not\equiv 1 \pmod{31},$$

$$a^{10}\not\equiv 1 \pmod{31},$$

$$a^{6}\not\equiv 1 \pmod{31}.$$

Kadangi, pavyzdžiui, $2^5=32\equiv 1 \pmod{31}$, tai ir

$$2^{10}\equiv 1 \pmod{31}.$$

Todėl skaičius 2^5 nėra primityvioji šaknis moduliu 31.

Uždaviniai

1. Raskite skaičių a, $10\leqslant a\leqslant 20$, rodiklius moduliais 13, 17, 21, 23 (tais atvejais, kai tie rodikliai egzistuoja).
2. Raskite skaičiaus a, $1<a<20$, $(a, m)=1$, rodiklius moduliais 16, 17, 18, 19, 20, 21.
3. Raskite, kiek liekanų klasių ir kokios turi rodiklį 9 moduliu 19.
4. Raskite visas primityviąsias šaknis moduliais 14, 15, 17, 18, 19, 21.
5. Nustatykite, kada a yra primityvioji šaknis moduliais 49, 50, 51, 53, 54, 55.
6. Raskite primityviąsias šaknis moduliais 6, 18, 54, 10, 50.

§44. Primityviųjų šaknų egzistavimas pirminiu moduliu

Simboliu $\psi(\delta)$ žymėsime skaičių liekanų klasių tam tikru moduliu su rodikliu δ tuo pačiu moduliu. Kadangi yra $\varphi(m)$ tarpusavyje pirminių su moduliu m liekanų klasių, kurioms apibrėžiamas rodiklis, tai

$$\sum_{\delta}\psi(\delta)=\varphi(m).$$

Įsitikinome, kad rodiklis moduliu m yra $\varphi(m)$ daliklis, taigi anksčiau užrašytą lygybę galime patikslinti:

$$\sum_{\delta\mid\varphi(m)}\psi(\delta)=\varphi(m). \tag{5.4}$$

Kai modulis m yra pirminis, t. y. $m=p$,

$$\sum_{\delta\mid(p-1)}\psi(\delta)=p-1.$$

78 teorema. *Egzistuoja* $\varphi(p-1)$ *primityviųjų šaknų pirminiu moduliu* p.

Įrodymas. Primityviosios šaknys moduliu p yra lyginio

$$x^{p-1} \equiv 1 \pmod{p}$$

sprendiniai. Iš pradžių nagrinėsime bet kurio laipsnio analogiškus lyginius.

Skaičius a, kurio rodiklis moduliu p lygus δ, yra lyginio

$$x^{\delta} \equiv 1 \pmod{p} \tag{5.5}$$

sprendinys, todėl skaičiai

$$a^0,\ a^1,\ a^2,\ \ldots,\ a^{\delta-1} \tag{5.6}$$

atstovauja visiems skirtingiems to lyginio sprendiniams. Iš tikrųjų pagal 74 teoremą tie skaičiai priklauso skirtingoms liekanų klasėms moduliu p. Pagal 64 teoremą (5.5) lyginys negali turėti daugiau kaip δ sprendinių. Tačiau (5.6) sekoje ne visų skaičių rodiklis yra δ. Būtent, jeigu $(k,\ \delta)=d>1$, tai

$$(a^k)^{\delta/d}=(a^{\delta})^{k/d} \equiv 1 \pmod{p}$$

ir $r\,(a^k) \leqslant \delta/d < \delta$. Taigi ieškant (5.5) lyginio sprendinių, kurių rodiklis moduliu p būtų δ, reikia iš (5.6) sekos išbraukti visus tuos a laipsnius a^k, kurių $(k,\ \delta)>1$. Liks $\varphi(\delta)$ skaičių. Todėl

$$\psi(\delta) \leqslant \varphi(\delta).$$

30 paragrafe pateikėme Oilerio funkcijos sumavimo formulę, kuri, kai $m=p-1$, yra šitokia:

$$\sum_{\delta \mid (p-1)} \varphi(\delta)=p-1.$$

Iš tos lygybės panariui atėmę (5.4) lygybę, gauname

$$\sum_{\delta \mid (p-1)} \big(\varphi(\delta)-\psi(\delta)\big)=0.$$

Tačiau $\varphi(\delta)-\psi(\delta)$ yra neneigiamas sveikasis skaičius. Tokių skaičių suma lygi nuliui, kai visi dėmenys yra nuliai:

$$\varphi(\delta)-\psi(\delta)=0,$$

$$\psi(\delta)=\varphi(\delta). \tag{5.7}$$

Ta lygybė įdomi ir pati savaime. Ji rodo, kad liekanų klasių bet kuriuo pirminiu moduliu su rodikliu δ tuo moduliu, yra $\varphi(\delta)$.

Imdami $\delta=p-1=\varphi(p)$, randame, kad primityviųjų šaknų moduliu p yra $\varphi(p-1)$.

Pavyzdžiai. 1. Patikrinsime Oilerio funkcijos sumavimo formulę, kai $m=12$. Skaičiaus $m=12$ natūriniai dalikliai yra 1, 2, 3, 4, 6, 12. Kadangi

$$\varphi(1)=1,\ \varphi(2)=1,\ \varphi(3)=2,\ \varphi(4)=2,\ \varphi(6)=2,\ \varphi(12)=4,$$

tai

$$\sum_{\delta \mid 12} \varphi(\delta) = 1+1+2+2+2+4 = 12.$$

2. Kiek yra primityviųjų šaknų moduliu 11.
Kadangi $\varphi(p-1) = \varphi(10) = 4$, tai šiuo moduliu yra 4 primityviosios šaknys.

Uždaviniai

7. Kiek yra primityviųjų šaknų šiais pirminiais moduliais:
1) $p=41$; 2) $p=53$; 3) $p=71$; 4) $p=97$; 5) $p=101$.

8. Raskite mažiausią primityviąją šaknį šiais moduliais:
1) $p=19$; 2) $p=23$; 3) $p=31$; 4) $p=43$; 5) $p=53$.

§45. Primityviosios šaknys sudėtiniu moduliu

Jeigu modulis yra sudėtinis skaičius, tai primityviųjų šaknų egzistavimo įrodymai žymiai sudėtingesni (žr. vadovėlio 1-ąjį leidimą). Apsiribosime tik bendromis pastabomis, į įrodymus nesigilinsime.

Bet kuri primityvioji šaknis moduliu p^α (pirminio skaičiaus natūriniu laipsniu α) kartu yra ir primityvioji šaknis moduliu p. Atvirkščias teiginys ne visuomet teisingas. Kad primityvioji šaknis a moduliu p būtų primityvioji šaknis ir moduliu p^α ($\alpha \geqslant 2$), turi būti išpildoma sąlyga

$$a^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}. \tag{5.8}$$

Pavyzdžiui, skaičius 3 yra primityvioji šaknis moduliu 7. Kad šis skaičius būtų primityvioji šaknis moduliu $49 = 7^2$, turi būti teisinga sąlyga

$$3^{7^0 \cdot 6} \not\equiv 1 \pmod{7^2}.$$

Kadangi

$$3^6 = 729 \not\equiv 1 \pmod{49},$$

tai 3 yra primityvioji šaknis ir moduliu 49, nes (5.8) sąlyga tenkinama.

Jeigu a — primityvioji šaknis moduliu p, tai bent vienas iš skaičių a ir $a+p$ yra primityvioji šaknis moduliu p^2, kai $p>2$.

Jeigu a yra primityvioji šaknis moduliu p^2, p — nelyginis pirminis skaičius, tai a — primityvioji šaknis ir visais aukštesniais p laipsniais.

Bet kuri nelyginė primityvioji šaknis moduliu p^α yra primityvioji šaknis ir moduliu $2p^\alpha$; čia p — nelyginis pirminis skaičius.

Jeigu a — nelyginis skaičius ir $a \geqslant 3$, tai a negali būti primityvioji šaknis moduliu 2.

Tiek žinių apie primityviąsias šaknis sudėtiniais moduliais. Beje, ne kiekvienu sudėtiniu moduliu tos šaknys egzistuoja. Jų egzistavimo atvejus nusako ši teorema.

79 teorema. *Primityviosios šaknys egzistuoja tik šitokiais moduliais* m:

$$m = 2,\ 4,\ p^\alpha,\ 2p^\alpha; \tag{5.9}$$

čia p *— nelyginis pirminis skaičius,* α *— natūrinis skaičius.*

Pavyzdys. Rasime, kuriais iš modulių 24, 25, 26, 27, 28 egzistuoja primityviosios šaknys. Užrašysime tų modulių kanoninius skaidinius:

$$24=2^3\cdot 3,\ 25=5^2,\ 26=2\cdot 13,\ 27=3^3,\ 28=2^2\cdot 7.$$

Remdamiesi 79 teorema, nustatome, kad moduliai 23 ir 24 nėra (5.9) tipo ir todėl tais moduliais nėra primityviųjų šaknų. Visais kitais moduliais primityviosios šaknys egzistuoja.

§46. Indeksai

Daugelyje matematikos sričių, ypač skaičiavimo uždaviniuose, plačiai taikomi logaritmai. Juos taikant, sudėtingesnės skaičiavimų operacijos – daugyba ir dalyba pakeičiamos paprastesnėmis – sudėtimi ir atimtimi.

Priminsime, kad skaičiaus a logaritmu pagrindu $g>1$ vadinamas toks laipsnio rodiklis k, su kuriuo teisinga lygybė

$$g^k=a.$$

Logaritmas žymimas $k=\log_g a$.

Logaritmo sąvokos analogas lyginių teorijoje yra *indeksas.*

Skaičiaus a, tarpusavyje pirminio su moduliu m, indeksu pagrindu g vadinamas toks neneigiamas skaičius k, su kuriuo

$$g^k\equiv a\ (\mathrm{mod}\ m).$$

Kadangi $(a, m)=1$, tai toks lyginys teisingas, kai $(g, m)=1$. Todėl indekso pagrindas ir modulis m turi būti tarpusavyje pirminiai skaičiai. Indeksas žymimas

$$k=\mathrm{ind}_g a.$$

Nagrinėsime, kokiomis sąlygomis gali egzistuoti indeksai.

80 teorema. *Visiems skaičiams, tarpusavyje pirminiams su moduliu m, egzistuoja indeksai pagrindu, lygiu primityviajai šakniai g moduliu m.*

Įrodymas. Pagal 74 teoremą skaičiai

$$g^0,\ g^1,\ g^2,\ \ldots,\ g^{\varphi(m)-1}$$

priklauso skirtingoms liekanų klasėms moduliu m. Kai $k>0$, iš sąryšio $(g, m)=1$ išplaukia sąryšis $(g^k, m)=1$. Taigi tie skaičiai atstovauja visoms $\varphi(m)$ liekanų klasėms, tarpusavyje pirminėms su moduliu. Vadinasi, bet kuris sveikasis skaičius a, $(a, m)=1$, lygsta vienam iš nurodytųjų g laipsnių:

$$a\equiv g^k\ (\mathrm{mod}\ m),\ 0\leqslant k\leqslant\varphi(m)-1.$$

Išvada. *Bet kurio tarpusavyje pirminio su moduliu skaičiaus a indeksas yra skaičius k, ne didesnis už $\varphi(m)-1$.*

Toliau nagrinėdami indeksus, raide g visur žymėsime kurią nors primityviąją šaknį nagrinėjamuoju moduliu. Indekso žymėjime pagrindą g taip pat kartais praleisime, t. y. vietoje $\operatorname{ind}_g a$ rašysime $\operatorname{ind} a$.

81 teorema. *Jeigu skaičiai* $a_1, a_2, \ldots, a_s$ *tarpusavyje pirminiai su moduliu* m, *tai*

$$\operatorname{ind}_g (a_1 a_2 \ldots a_s) = \sum_{i=1}^{s} \operatorname{ind}_g (a_i) \left(\operatorname{mod} \varphi (m)\right). \tag{5.10}$$

Įrodymas. Pagal indekso apibrėžimą

$$\begin{aligned} a_1 a_2 \ldots a_s &\equiv g^{\operatorname{ind} a_1 a_2 \ldots a_s} (\operatorname{mod} m), \\ a_1 &\equiv g^{\operatorname{ind} a_1} (\operatorname{mod} m), \\ a_2 &\equiv g^{\operatorname{ind} a_2} (\operatorname{mod} m), \\ &\ldots\ldots\ldots\ldots \\ a_s &\equiv g^{\operatorname{ind} a_s} (\operatorname{mod} m). \end{aligned}$$

Sudauginę paskutinius s lyginių, gauname

$$g^{\operatorname{ind} a_1 a_2 \ldots a_s} \equiv g^{\sum_{i=1}^{s} \operatorname{ind} a_i} (\operatorname{mod} m).$$

Dabar teoremos teiginys išplaukia iš 75 teoremos.

Išvada.

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \left(\operatorname{mod} \varphi (m)\right).$$

82 teorema. $a \equiv b \pmod m \Leftrightarrow \operatorname{ind}_g a \equiv \operatorname{ind}_g b \left(\operatorname{mod} \varphi (m)\right)$.

Įrodymas analogiškas 81 teoremos įrodymui. Jeigu

$$\begin{aligned} a &\equiv g^{\operatorname{ind} a} (\operatorname{mod} m), \\ b &\equiv g^{\operatorname{ind} b} (\operatorname{mod} m), \end{aligned}$$

tai iš čia

$$g^{\operatorname{ind} a} \equiv g^{\operatorname{ind} b} (\operatorname{mod} m),$$

ir vėl telieka remtis 75 teorema.

Atvirkščiai, jeigu $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{\varphi (m)}$, tai $\operatorname{ind} a = \operatorname{ind} b + \varphi (m) t$,

$$a \equiv g^{\operatorname{ind} a} \equiv g^{\operatorname{ind} b + \varphi (m) t} \equiv g^{\operatorname{ind} b} \equiv b \pmod m.$$

83 teorema. *Jeigu* g *yra nelyginė primityvioji šaknis moduliu* p^α, p *— nelyginis pirminis skaičius,* $(a, 2p) = 1$, *tai kiekvienas skaičiaus* a *indeksas* k *pagrindu* g *ir moduliu* p^α *yra to paties skaičiaus indeksas pagrindu* g *ir moduliu* $2p^\alpha$.

Įrodymas. Iš teoremos sąlygų turime

$$g^k \equiv a \pmod{p^\alpha}.$$

Kadangi g ir a — nelyginiai skaičiai, tai

$$g^k \equiv a \pmod{2}.$$

Iš tų dviejų lyginių gauname

$$g^k \equiv a \pmod{2p^\alpha}.$$

Matome, kad indeksus galime sudaryti visais moduliais, kuriais egzistuoja primityviosios šaknys. Nustatėme, kad tos pačios liekanų klasės moduliu m skaičiai turi tą pačią indeksų liekanų klasę moduliu $\varphi(m)$. Iš 80 teoremos išvados išplaukia, kad indeksais pakanka parinkti mažiausius neneigiamus tų klasių skaičius. Indeksų taisyklės panašios į logaritmų taisykles: sandaugos indeksas lygsta dauginamųjų indeksų sumai moduliu $\varphi(m)$, laipsnio rodiklis nukeliamas prieš indekso ženklą.

Iš 80 teoremos išplaukia, kad nuo skaičių lyginių moduliu m galima pereiti prie jų indeksų lyginių moduliu $\varphi(m)$ ir atvirkščiai. Abu tie veiksmai vadinami *atitinkamai indeksavimu* ir *antiindeksavimu.*

Dar kartą priminsime, kad negalima užmiršti modulio pasikeitimo indeksuojant ir antiindeksuojant:

indeksuojant modulis m keičiamas $\varphi(m)$,

antiindeksuojant modulis $\varphi(m)$ keičiamas m.

Pavyzdžiai. 1. Praeitame paragrafe nustatėme, kad 3 yra primityvioji šaknis moduliu 7. Išreikšime 3 laipsniais visus už 7 mažesnius natūrinius skaičius:

$$1 \equiv 3^0 \pmod 7, \qquad 4 \equiv 3^4 \pmod 7,$$

$$2 \equiv 3^2 \pmod 7, \qquad 5 \equiv 3^5 \pmod 7,$$

$$3 \equiv 3^1 \pmod 7, \qquad 6 \equiv 3^3 \pmod 7.$$

Rastieji rodikliai ir yra kairiojoje lyginių pusėje esančių skaičių indeksai:

$$0 = \operatorname{ind}_3 1, \qquad 4 = \operatorname{ind}_3 4,$$
$$2 = \operatorname{ind}_3 2, \qquad 5 = \operatorname{ind}_3 5,$$
$$1 = \operatorname{ind}_3 3, \qquad 3 = \operatorname{ind}_3 6.$$

Praktiškai paprasčiau indeksus skaičiuoti keliant primityviąją šaknį visais iš eilės natūriniais skaičiais nuo 1 iki $p-1$.

2. Remdamiesi pirmojo pavyzdžio skaičiavimų rezultatais, tikrinsime 81 teoremos teiginį. Turime skaičių sandaugą $3 \cdot 5 \cdot 6 = 90$. Ieškome atskirų dauginamųjų ir visos sandaugos indeksų:

$$\operatorname{ind}_3 90 = \operatorname{ind}_3 (7 \cdot 12 + 6) = \operatorname{ind}_3 6 = 3,$$

$$\operatorname{ind}_3 (3 \cdot 5 \cdot 6) = \operatorname{ind}_3 3 + \operatorname{ind}_3 5 + \operatorname{ind}_3 6 = 1 + 5 + 3 = 9.$$

Kadangi $9 \equiv 3 \pmod 6$, tai

$$\operatorname{ind}_3 (3 \cdot 5 \cdot 6) \equiv \operatorname{ind}_3 3 + \operatorname{ind}_3 5 + \operatorname{ind}_3 6 \pmod 6.$$

3. Rasime, kurių skaičių indeksai lygūs nuliui. Kadangi g^0 lygsta 1 bet kuriuo moduliu, tai vienetinės bet kuriuo moduliu liekanų klasės skaičiai turi indeksą, lygų 0.

Kaip minėjome, indeksai sėkmingai taikomi sprendžiant kai kuriuos uždavinius. Tais atvejais labai praverčia indeksų lentelės.

Indeksų lentelių sudarymas. Konkrečiu pavyzdžiu parodysime, kaip sudaromos indeksų ir antiindeksų lentelės kuriuo nors moduliu.

Imsime $m=17$. Norėdami sudaryti indeksų lentelę, turime rasti primityviąją šaknį g tuo moduliu. Kadangi $\varphi(17)=16$, tai pagal 77 teoremą reikia rasti tokią g, kad

$$g^8 \not\equiv 1 \pmod{17}.$$

Patogiausia pradėti nuo mažesnių skaičių. Skaičius 1 nėra primityvioji šaknis jokiu moduliu $m>1$. Tikrinsime skaičių 2:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^4 \equiv -1,\ 2^8 \equiv 1 \pmod{17}.$$

Taigi skaičius 2 nėra primityvioji šaknis tuo moduliu. Toliau iš eilės tikriname skaičių 3:

$$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^4 \equiv -4,\ 3^8 \equiv -1 \pmod{17}.$$

Skaičius 3 tenkina primityviųjų šaknų kriterijų. Vadinasi, pagrindu 3 galima sudaryti indeksus. Keliame 3 visais laipsniais iki 15 imtinai:

$$3^1 \equiv 3,\ 3^5 \equiv 5,\ 3^9 \equiv 14,\ 3^{13} \equiv 12,$$

$$3^2 \equiv 9,\ 3^6 \equiv 15,\ 3^{10} \equiv 8,\ 3^{14} \equiv 2,$$

$$3^3 \equiv 10,\ 3^7 \equiv 11,\ 3^{11} \equiv 7,\ 3^{15} \equiv 6,$$

$$3^3 \equiv 13,\ 3^8 \equiv 16,\ 3^{12} \equiv 4,\ 3^{16} \equiv 3^0 \equiv 1 \pmod{17}$$

Paskutinis skaičiavimas (3^{16}) yra tik kontrolinis. Skaičiuojant 3 laipsnių liekanas, nebūtina ieškoti 3^k reikšmės, užtenka ankstesnio lyginio abi puses dauginti iš 3.

Pagal Oilerio teoremą $3^{16} \equiv 1 \pmod{17}$. Kadangi indeksai gali būti nustatomi mod $\varphi(17)$ = mod 16 tikslumu, tai patogiau skaičiaus 1 indeksu laikyti 0, o ne 16. Dabar belieka rastuosius skaičius surašyti į lentelę.

$g=3$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ind a	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Indeksų lentelė paprastai sudaroma šitaip: didėjimo tvarka nuo 1 iki $m-1$ išdėstomi liekanų klasių atstovai, o ties kiekvienu skaičiumi parašomas jo indeksas. Jeigu didėjimo tvarka išdėstysime indeksus, o ties jais parašysime skaičius, tai turėsime antiindeksų lentelę. Šiuo atveju antiindeksų lentelė būtų šitokia:

ind a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Knygos pabaigoje pateiktos indeksų lentelės visais pirminiais moduliais, ne didesniais už 100.

Uždaviniai

9. Sudarykite indeksų lenteles moduliais 11, 13, 19, 23, 29.
10. Sudarykite indeksų ir antiindeksų lenteles moduliais 25, 26, 27, 38, 50.
11. Nustatykite, kuriais dviženkliais moduliais galima sudaryti indeksų lenteles.

§47. Indeksų taikymai

Naudojantis indeksais, galima išspręsti dvinarius

$$ax^n \equiv b \pmod m$$

pavidalo lyginius tais moduliais, kuriais egzistuoja primityviosios šaknys.

84 teorema. *Jeigu moduliu m egzistuoja primityvioji šaknis g, o a ir m tarpusavyje pirminiai $(n, \varphi(m))=d$, tai lyginys*

$$ax^n \equiv b \pmod m$$

yra išsprendžiamas, kai

$$d \mid (\operatorname{ind}_g b - \operatorname{ind}_g a),$$

ir turi d sprendinių.

Įrodymas. Akivaizdu, kad sveikieji skaičiai x, kurie tenkina lyginį, turi būti tarpusavyje pirminiai su moduliu. Užrašysime visų skaičių a, b, x indeksus:

$$a \equiv g^{\operatorname{ind} a} \pmod m,$$

$$b \equiv g^{\operatorname{ind} b} \pmod m,$$

$$x \equiv g^{\operatorname{ind} x} \pmod m.$$

$$ax^n \equiv b \pmod m \Rightarrow g^{\operatorname{ind} a + n \operatorname{ind} x} \equiv g^{\operatorname{ind} b} \pmod m.$$

Iš čia, remdamiesi 81 teorema, gauname

$$\operatorname{ind} a + n \operatorname{ind} x \equiv \operatorname{ind} b \left(\operatorname{mod} \varphi(m)\right),$$

$$ny \equiv \operatorname{ind} b - \operatorname{ind} a \left(\operatorname{mod} \varphi(m)\right);$$

čia $y=\operatorname{ind} x$. Pastarasis lyginys yra pirmojo laipsnio y atžvilgiu. Jo išsprendžiamumo sąlygos sutampa su įrodomosios teoremos sąlygomis.

Naudojantis indeksais, ypač patogu spręsti dvinarius lyginius pirminiu moduliu p, kai yra sudaryta indeksų lentelė tuo moduliu. Taip pat galima spręsti ir rodiklinius lyginius

$$ca^x \equiv f \pmod{p},$$

kai skaičiai c, a, f – tarpusavyje pirminiai su pirminiu p. Indeksuodami tą lyginį, gauname

$$x \operatorname{ind} a \equiv \operatorname{ind} f - \operatorname{ind} c \pmod{p-1}.$$

Šis lyginys yra pirmojo laipsnio, jo sprendinys moduliu $p-1$ egzistuoja tada ir tik tada, kai

$$(\operatorname{ind} a,\ p-1) \mid (\operatorname{ind} f - \operatorname{ind} c)$$

(žr. 58 teoremą).

Turint indeksų lentelę pirminiu moduliu p, nesunku nustatyti, kurie skaičiai yra kvadratinės liekanos tuo moduliu. Tarkime, kad išsprendžiamas lyginys

$$x^2 \equiv a \pmod{p}.$$

Indeksuodami šį lyginį, gauname

$$2 \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}.$$

Taigi kvadratinės liekanos indeksas turi būti lyginis skaičius, nes $p-1$ yra lyginis skaičius, kai $p>2$.

Pavyzdžiai. 1. Išspręsime lyginį

$$7x^{12} \equiv 10 \pmod{17}.$$

Tą lyginį indeksuojame:

$$\operatorname{ind} 7 + 12 \operatorname{ind} x \equiv \operatorname{ind} 10 \pmod{16},$$

$$12 \operatorname{ind} x \equiv \operatorname{ind} 10 - \operatorname{ind} 7 \pmod{16}.$$

Iš ankstesniame paragrafe sudarytos indeksų lentelės moduliu 17 (tuo moduliu, kuriuo turime lyginį prieš indeksavimą) randame

$$\operatorname{ind} 10 = 3, \quad \operatorname{ind} 7 = 11.$$

Todėl

$$12 \operatorname{ind} x \equiv -8 \pmod{16}.$$

Kadangi $(12, 16) = 4$, $4 \mid -8$, tai tas lyginys išsprendžiamas ir turi 4 sprendinius. Juos rasime šitaip:

$$3 \operatorname{ind} x \equiv -2 \pmod{4},$$

$$3 \operatorname{ind} x \equiv -2 + 2 \cdot 4 \pmod{4},$$

$$\operatorname{ind} x \equiv 2 \pmod{4}.$$

Antiindeksuojant nuo lyginio moduliu $\varphi(m)$ grįžtama prie lyginio moduliu m, todėl ir sprendžiamojo lyginio sprendinius būtinai reikia užrašyti moduliu 16. Taigi

$$\operatorname{ind} x_1 \equiv 2 \pmod{16},$$

$$\operatorname{ind} x_2 \equiv 6 \pmod{16},$$

$$\operatorname{ind} x_3 \equiv 10 \pmod{16},$$

$$\operatorname{ind} x_4 \equiv 14 \pmod{16}.$$

Antiindeksuodami tuos 4 lyginius, t. y. iš indeksų lentelės rasdami skaičiaus x reikšmes, kai žinomos ind x reikšmės, gauname

$$x_1 \equiv 9 \pmod{17},$$

$$x_2 \equiv 15 \pmod{17},$$

$$x_3 \equiv 8 \pmod{17},$$

$$x_4 \equiv 2 \pmod{17}.$$

Tai ir yra visi lyginio $7x^{12} \equiv 10 \pmod{17}$ sprendiniai.

2. Naudodamiesi indeksais, rasime pirmojo laipsnio lyginio

$$15x \equiv 11 \pmod{17}$$

sprendinius. Indeksuodami ir antiindeksuodami gauname:

$$\text{ind } 15 + \text{ind } x \equiv \text{ind } 11 \pmod{16},$$

$$\text{ind } x \equiv \text{ind } 11 - \text{ind } 15 \pmod{16},$$

$$\text{ind } x \equiv 7 - 6 \equiv 1 \pmod{16},$$

$$x \equiv 3 \pmod{17}.$$

3. Naudodamiesi indeksais, rasime rodiklinio lyginio

$$10 \cdot 7^x \equiv 13 \pmod{17}$$

sprendinį. Indeksuojame:

$$\text{ind } 10 + x \text{ ind } 7 \equiv \text{ind } 13 \pmod{16}.$$

$$11x \equiv 4 - 3 \pmod{16},$$

$$11x \equiv 1 \pmod{16},$$

$$11x \equiv 1 + 2 \cdot 16 \pmod{16},$$

$$x \equiv 3 \pmod{16}.$$

Rodiklinio lyginio sprendiniai pagal 82 teoremą yra liekanų klasės moduliu $\varphi(m)$, šiuo atveju moduliu 16. Sprendžiant tokius lyginius, antiindeksuoti nereikia.

4. Rasime skaičiaus 14 rodiklį moduliu 17. Rodiklis yra mažiausias teigiamas δ, su kuriuo teisinga sąlyga

$$14^{\delta} \equiv 1 \pmod{17}.$$

Indeksuojame:

$$\delta \text{ ind } 14 \equiv 0 \pmod{16},$$

$$9\delta \equiv 0 \pmod{16},$$

$$\delta \equiv 0 \pmod{16},$$

$$\delta = 16t;$$

čia t — sveikasis skaičius. Mažiausia teigiama δ reikšmė gaunama parinkus $t=1$. Taigi

$$r(14) = 16.$$

Vadinasi, skaičius 14 yra primityvioji šaknis moduliu 17.

5. Rasime skaičiaus 13^{100} dalybos iš 17 liekaną. Sprendžiame lyginį $13^{100} \equiv x \pmod{17}$:

$$100 \text{ ind } 13 \equiv \text{ind } x \pmod{16},$$

$$\text{ind } x \equiv 400 \pmod{16},$$

$$\text{ind } x \equiv 0 \pmod{16},$$

$$x \equiv 1 \pmod{17}.$$

Dalybos liekana lygi 1.

6. Išspręsime lyginį sudėtiniu moduliu 18:

$$7x^{10} \equiv 13 \pmod{18}.$$

Indeksuojame:

$$\operatorname{ind} 7 + 10 \operatorname{ind} x \equiv \operatorname{ind} 13 \pmod 6,$$

nes $\varphi(18) = 6$. Toliau sprendžiame žinomu būdu:

$$10 \operatorname{ind} x \equiv 4 - 2 \equiv 2 \pmod 6,$$

$$4 \operatorname{ind} x \equiv 2 \pmod 6.$$

Lyginys turi 2 sprendinius, nes $(4, 6) = 2$.

$$2 \operatorname{ind} x \equiv 1 \pmod 3,$$

$$\operatorname{ind} x \equiv 2 \pmod 3,$$

$$\operatorname{ind} x_1 \equiv 2 \pmod 6,$$

$$\operatorname{ind} x_2 \equiv 5 \pmod 6.$$

Antiindeksuojame:

$$x_1 \equiv 7 \pmod{18},$$

$$x_2 \equiv 11 \pmod{18}.$$

7. Išspręsime lyginį

$$11x^{16} \equiv 7 \pmod{18};$$

$$\operatorname{ind} 11 + 16 \operatorname{ind} x \equiv \operatorname{ind} 7 \pmod 6,$$

$$16 \operatorname{ind} x \equiv 2 - 5 \pmod 6,$$

$$16 \operatorname{ind} x \equiv -3 \pmod 6.$$

Tas lyginys sprendinių neturi, nes $(16, 6) = 2$, $2 \nmid -3$.

Turint indeksų lentelę pirminiu moduliu p, galima rasti visas primityviąsias šaknis tuo moduliu.

Tarkime, kad indeksų lentelei sudaryti pasirinkome primityviąją šaknį g. Sprendžiame lyginį

$$a^x \equiv 1 \pmod p.$$

Indeksuodami tą lyginį (pagrindu g), gauname

$$x \operatorname{ind}_g a \equiv 0 \pmod{p-1}.$$

Matome, kad kairiojoje lyginio pusėje esanti sandauga yra $p-1$ kartotinis. Iš žinomų lyginių savybių galime daryti išvadą, kad mažiausia natūrinė x reikšmė, su kuria tas lyginys teisingas, yra

$$x = \frac{p-1}{d};$$

čia

$$d = (\operatorname{ind}_g a,\ p-1).$$

Vadinasi, skaičiaus a rodiklis moduliu p lygus $p-1$, kai $d=1$. Savo ruožtu, kaip matome, $d=1$, kai skaičiaus a indeksas pagrindu g tarpusavyje pirminis su $p-1$.

Peržvelgę anksčiau sudarytą indeksų lentelę moduliu $p=17$, matome, kad su skaičiumi 16 tarpusavyje pirminiai yra šių skaičių indeksai: 3, 5, 6, 7, 10, 11, 12, 14. Taigi visi tie skaičiai yra primityviosios šaknys moduliu 17. Beje, jų yra tiek, kiek ir nurodyta 76 teoremos išvadoje: $\varphi(16)=8$.

Uždaviniai

Naudodamiesi indeksais, išspręskite šiuos lyginius.

12. $x^{12}\equiv -4 \pmod{41}$, $x^{27}\equiv 28 \pmod{47}$,
$x^{6}\equiv 7 \pmod{41}$, $x^{49}\equiv 100 \pmod{31}$,
$x^{3}\equiv 15 \pmod{41}$, $x^{24}\equiv 28 \pmod{29}$.

13. $18x^{13}\equiv 71 \pmod{19}$, $49x^{65}\equiv 9 \pmod{71}$,
$50x^{17}\equiv 49 \pmod{53}$, $37x^{38}\equiv 39 \pmod{79}$,
$59x^{30}\equiv 14 \pmod{73}$, $12x^{41}\equiv 41 \pmod{43}$.

14. $121x\equiv 100 \pmod{73}$, $137x\equiv 1 \pmod{53}$,
$91x\equiv 15 \pmod{71}$, $79x\equiv 83 \pmod{97}$,
$50x\equiv 61 \pmod{67}$, $13x\equiv 23 \pmod{43}$.
$20^{x}\equiv 21 \pmod{41}$, $8^{x}\equiv 17 \pmod{59}$,
$43^{x}\equiv -14 \pmod{31}$, $12^{x}\equiv 100 \pmod{67}$,
$(-9)^{x}\equiv 99 \pmod{61}$, $32^{x}\equiv 16 \pmod{71}$.

15. Naudodamiesi indeksais, raskite visų liekanų klasių, tarpusavyje pirminių su moduliu, rodiklius moduliais 23, 29, 31, 37, 39.

16. Naudodamiesi indeksais, raskite liekaną, dalydami 14^{50} iš 13, 7^{77} iš 19, 51^{100} iš 23, 15^{66} iš 29, 65^{401} iš 31.

§48. Sisteminės trupmenos

Remdamiesi nagrinėtomis laipsninių liekanų savybėmis, galime rasti trupmenų periodo ilgį.

Kiekvieną realųjį skaičių α galima išreikšti jo sveikosios ir trupmeninės dalies suma: $\alpha=[\alpha]+\{\alpha\}$.

Trupmeninė dalis $\{\alpha\}$ yra intervalo $[0, 1)$ skaičius. Tą skaičių, pasirinkus tam tikrą natūrinį skaičių $g>1$, galima užrašyti šitaip:

$$\{\alpha\}=\frac{b_1}{g}+\frac{b_2}{g^2}+\ldots+\frac{b_k}{g^k}+\ldots;$$

čia b_i — neneigiami sveikieji skaičiai, mažesni už g:

$$0\leqslant b_i<g.$$

Pastaroji trupmena vadinama *sistemine trupmena pagrindu g*. Jeigu $g=10$, tai turime įprastinę dešimtainę trupmeną.

Sisteminė trupmena gali būti *baigtinė* (kai skaičių b_i seka baigtinė) ir *begalinė* (kai ta seka begalinė).

Begalinės sisteminės trupmenos skirstomos į *periodines* ir *neperiodines*.

Begalinę sisteminę trupmeną patogiau žymėti

$$\sum_{i=1}^{\infty} b_i g^{-i}.$$

Begalinė sisteminė trupmena

$$\sum_{i=1}^{\infty} b_i g^{-i}$$

vadinama periodine, kai yra tokie natūriniai skaičiai m ir k, su kuriais teisingos lygybės

$$b_{m+n+k}=b_{m+n} \quad (\forall n \in \mathbf{N}).$$

Skaičius m vadinamas *priešperiodžio ilgiu*, k – *periodo ilgiu*. Kai $m=0$, trupmena vadinama *grynąja periodine*, priešingu atveju – *mišriąja periodine trupmena*.

Iš šių apibrėžimų išplaukia, kad mišriosios periodinės trupmenos skaitmenų seka yra periodinė:

$$b_1, \ldots, b_m, b_{m+1}, \ldots, b_{m+k}, b_{m+k+1}, \ldots, b_{m+2k}, \ldots$$

Baigtinę sisteminę trupmeną žymėsime

$$\sum_{i=1}^{n} b_i g^{-i}=0, b_1 b_2 \ldots b_{n(g)}.$$

Periodinė sisteminė trupmena, turinti m ilgio priešperiodį ir k ilgio periodą, žymima šitaip:

$$\sum_{i=1}^{\infty} b_i g^{-i}=0, b_1 b_2 \ldots b_m (\overline{b_{m+1} \ldots b_{m+k}})_{(g)}.$$

Kiekvieną tokią trupmeną galime išreikšti racionaliuoju skaičiumi. Sugrupuokime trupmenos dėmenis šitaip:

$$\begin{aligned}\sum_{i=1}^{\infty} b_i g^{-i} &= b_1 g^{-1}+\ldots+b_m g^{-m}+g^{-m}(b_{m+1} g^{-1}+\ldots+\\ &+b_{m+k} g^{-k})+g^{-m-k}(b_{m+1} g^{-1}+\ldots+b_{m+k} g^{-k})+\ldots+\\ &+g^{-m-jk}(b_{m+1} g^{-1}+\ldots+b_{m+k} g^{-k})+\ldots=\\ &=g^{-m}(b_1 g^{m-1}+\ldots+b_m+g^{-k}(b_{m+1} g^{k-1}+\ldots+b_{m+k})+\\ &+g^{-2k}(b_{m+1} g^{k-1}+\ldots+b_{m+k})+\ldots+\\ &+g^{-jk}(b_{m+1} g^{k-1}+\ldots+b_{m+k})+\ldots).\end{aligned}$$

Pažymėję

$$A=\overline{b_1 b_2 \ldots b_{m(g)}},$$

$$B=\overline{b_{m+1} b_{m+2} \ldots b_{m+k(g)}},$$

turime:

$$\sum_{i=1}^{\infty} b_i g^{-i} = g^{-m}\left(A + B\sum_{j=1}^{\infty} g^{-jk}\right) = g^{-m}\left(A + B\,\frac{1}{g^k - 1}\right).$$

Kartu išvedėme formulę, kuria naudodamiesi periodinę sisteminę trupmeną galime užrašyti paprastąja trupmena.

Pavyzdžiui, pagal šią formulę periodinę dešimtainę trupmeną 0,42(531) išreiškiame trupmena

$$0{,}42\,(531) = \frac{1}{100}\left(42 + \frac{531}{999}\right).$$

Nagrinėsime dėsningumus, išryškėjančius skleidžiant racionaliuosius skaičius sisteminėmis trupmenomis.

85 teorema. *Būtina ir pakankama sąlyga, kad nesuprastinamą trupmeną a/b būtų galima užrašyti baigtine sistemine trupmena pagrindu g, — visi trupmenos vardiklio b pirminiai dalikliai turi būti ir sistemos pagrindo dalikliai.*

Jeigu $0 < a < b$, $(a, b) = (g, b) = 1$, tai trupmena a/b išskleidžiama grynąja periodine sistemine trupmena pagrindu g. Periodo ilgis lygus skaičiaus g rodikliui k moduliu b.

Įrodymas. Iš pradžių įrodysime pirmąjį teoremos teiginį. Jeigu $(a, b) = 1$ ir

$$\frac{a}{b} = \frac{N}{g^k},$$

tai $ag^k = bN$. Jeigu skaičius b dalijasi iš pirminio skaičiaus p, tai ir skaičius ag^k dalijasi iš p. Tačiau p negali būti skaičiaus a daliklis, todėl $p \mid g^k$. Iš čia $p \mid g$. Įrodėme teoremos pirmojo teiginio sąlygos būtinumą. Dabar įrodysime jos pakankamumą.

Jeigu skaičiaus g kanoninis skaidinys yra

$$g = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

o b savo kanoniniame skaidinyje neturi kitokių pirminių daugiklių, tai b galime užrašyti šitaip:

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k};$$

čia kai kurie β_i gali būti lygūs nuliui. Atitinkamai parinkę daugiklį c, galime užrašyti $bc = g^m$.

Iš tikrųjų, jeigu

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k},$$

tai sąlyga $bc = g^m$ ekvivalenti k lygčių

$$\beta_i + \gamma_i = m\alpha_i$$

($i=1, 2, \ldots, k$) sistemai. Tačiau k tiesinių lygčių su $k+1$ kintamuoju m, $\gamma_1, \gamma_2, \ldots, \gamma_k$ sistema visuomet išsprendžiama ir turi nenulinį sprendinį. Taigi toks skaičius c egzistuoja ir

$$\frac{a}{b}=\frac{ac}{bc}=\frac{ac}{g^m}.$$

Skaičių ac galime užrašyti sisteminiu sveikuoju skaičiumi pagrindu g. Visus šio sisteminio skaičiaus laipsnius padaliję iš g^m, gausime trupmenos a/b išraišką sistemine trupmena pagrindu g.

Pirmasis teoremos teiginys įrodytas. Įrodysime antrąjį teiginį.

Parašykime štai tokias dalybos iš b su liekana lygybes:

$$\begin{aligned} ga &= bc_1 + r_1, \\ gr_1 &= bc_2 + r_2, \\ gr_2 &= bc_3 + r_3, \\ &\cdots\cdots\cdots \\ gr_{k-1} &= bc_k + r_k. \end{aligned} \tag{5.11}$$

Kadangi

$$(a, b)=(b, r_1)=(r_1, r_2)=\ldots=(r_{k-1}, r_k),$$

tai $r_i>0$. Visos liekanos r_i yra teigiamos ir mažesnės už b . Tačiau iš sąlygų $a<b$ ir $r_i<b$ išplaukia, kad $0\leqslant c_i<g$.

Padalykime pirmąją iš (5.11) lygybių iš gb, antrąją iš g^2b, trečiąją iš g^3b ir t. t., paskutinę iš g^kb. Gausime šitokias lygybes:

$$\begin{aligned} \frac{a}{b} &= \frac{c_1}{g}+\frac{r_1}{bg}, \\ \frac{r_1}{bg} &= \frac{c_2}{g^2}+\frac{r_2}{bg^2}, \\ &\cdots\cdots\cdots\cdots \\ \frac{r_{k-1}}{bg^{k-1}} &= \frac{c_k}{g^k}+\frac{r_k}{bg^k}. \end{aligned}$$

Panariui sudėję gautąsias lygybes, turime

$$\frac{a}{b}=\frac{c_1}{g}+\frac{c_2}{g^2}+\ldots+\frac{c_k}{g^k}+\frac{r_k}{bg^k},$$

arba

$$ag^k=c_1g^{k-1}b+c_2g^{k-2}b+\ldots+c_kb+r_k.$$

Iš pastarosios lygybės gauname

$$ag^k\equiv r_k \pmod b.$$

Pagal rodiklio k apibrėžimą $g^k\equiv 1 \pmod b$, taigi

$$a\equiv r_k \pmod b.$$

Abu skaičiai a ir r_k yra neneigiami ir mažesni už b, todėl tas lyginys galimas tik tada, kai $a=r_k$. Gauname

$$\frac{a}{b}=\frac{c_1}{g}+\frac{c_2}{g^2}+\ldots+\frac{c_k}{g^k}+\frac{a}{b}\cdot\frac{1}{g^k}.$$

Dešiniojoje lygybės pusėje trupmeną a/b pakeitę visa dešiniosios lygybės pusės reikšme, gauname

$$\frac{a}{b}=\frac{c_1}{g}+\frac{c_2}{g^2}+\ldots+\frac{c_k}{g^k}+\frac{c_1}{g^{k+1}}+\ldots+\frac{c_k}{g^{2k}}+\frac{a}{b}\cdot\frac{1}{g^{2k}}.$$

Vietoj trupmenos a/b dešiniojoje lygybės pusėje vėl įrašę jos reikšmę, pastebime, kad skaičių c_1, c_2, ..., c_k rinkinys pradeda periodiškai kartotis. Įrodysime, kad to rinkinio negalima suskaidyti į keletą mažesnių periodinių rinkinių.

Iš tikrųjų, jeigu gautume

$$\frac{a}{b}=\frac{c_1}{g}+\frac{c_2}{g^2}+\ldots+\frac{c_s}{g^s}+\frac{a}{b}\cdot\frac{1}{g^s},$$

tai visai taip pat kaip ir anksčiau galėtume gauti lyginius

$$ag^s\equiv a\ (\mathrm{mod}\ b),$$
$$g^s\equiv 1\ (\mathrm{mod}\ b).$$

Tačiau tai prieštarauja prielaidai $r(g)=k$.

1 išvada. *Jeigu* $(a, b)=1$, $(b, g)=1$, *tai trupmenos periodo ilgis nepriklauso nuo skaitiklio* a *reikšmės.*

Iš tikrųjų pagal teoremą periodo ilgis yra $r_b(g)$.

2 išvada. *Sakykime, nesuprastinamos trupmenos vardiklis yra* $b=b_1b_2$; *čia daugiklis* b_2 *tarpusavyje pirminis su sistemos pagrindu* g, *daugiklis* b_1 *savo kanoniniame skaidinyje turi tik tuos pirminius daugiklius, iš kurių dalijasi* g. *Jeigu* g^r *yra mažiausias neneigiamas pagrindo* g *laipsnis, kuris dalijasi iš* b_1, *o* $r_g(b_2)=k$, *tai trupmeną* a/b *skleidžiant periodine sistemine trupmena pagrindu* g *gaunamas ilgio* r *priešperiodis ir ilgio* k *periodas.*

Įrodymas. Jeigu c yra toks daugiklis, kad $b_1c=g^r$, tai

$$\frac{a}{b}=\frac{a}{b_1b_2}=\frac{ac}{b_1cb_2}=\frac{ac}{g^rb_2}=\frac{1}{g^r}\left(A+\frac{d}{b_2}\right);$$

čia A – trupmenos $\frac{ac}{b_2}$ sveikoji dalis, $d<b_2$. Skaičius c savo kanoniniame skaidinyje turi tik tuos pirminius daugiklius, iš kurių dalijasi g, todėl $(c, b_2)=1$. Iš sąlygų $(a, b)=(c, b_2)=1$ išplaukia

$$(ac, b_2)=1\Rightarrow(d, b_2)=1.$$

Trupmena d/b_2 tenkina 85 teoremos sąlygas, taigi ji yra išskleidžiama grynąja periodine sistemine trupmena pagrindu g:

$$\frac{d}{b_2}=0,\overline{(c_1\,c_2\ldots c_k)}_{(g)}.$$

Jeigu skaičiaus A išraiška skaičiavimo sistemoje pagrindu g yra

$$A=\overline{d_1\,d_2\ldots d_n}_{(g)},$$

tai

$$A+\frac{d}{b_2}=\overline{d_1\,d_2\ldots d_n,\ (c_1\,c_2\ldots c_k)}_{(g)}.$$

To skaičiaus dalijimas iš g^r tolygus kablelio perkėlimui per r vienetų į kairę: nuo to periodo ilgis nesikeičia, tačiau sisteminė trupmena gali būti mišrioji periodinė. Priešperiodžio ilgis kaip tik ir lygus r.

Pavyzdžiai. 1. Skaičiaus $\frac{5}{12}$ vardiklis neturi pirminių daliklių, kurie nebūtų 6 dalikliai. Todėl tą trupmeną galima išskleisti baigtine sistemine trupmena pagrindu 6:

$$\frac{5}{12}=\frac{5}{2^2\cdot 3}=\frac{5\cdot 3}{2^2\cdot 3^2}=\frac{15}{6^2}=\frac{2\cdot 6+3}{6^2}=\frac{2}{6}+\frac{3}{6^2}=0,\overline{23}_{(6)}.$$

2. Rasime periodo ilgį skleisdami trupmeną 15/17 dešimtaine.
Tas ilgis lygus $\delta=r_{17}$ (10). Rasime tą skaičių naudodamiesi indeksais:

$$10^{\delta}\equiv 1 \pmod{17},$$
$$\delta \operatorname{ind} 10\equiv 0 \pmod{16},$$
$$3\delta\equiv 0 \pmod{16},$$
$$\delta\equiv 0 \pmod{16},$$
$$\delta=16t.$$

Minimali teigiama δ reikšmė yra 16. Taigi trupmenos 15/17 periodo ilgis lygus 16. Tokį pat periodo ilgį gauname skleisdami dešimtaine trupmena bet kurį racionalųjį skaičių $a/17$ kurio $(a,\ 17)=1$.

3. Rasime periodo ir priešperiodžio ilgį skleisdami trupmeną 2/15 šešetaine trupmena.
Kadangi $g=6$, tai 85 teoremos 2 išvadoje apibrėžti skaičiai b_1 ir b_2 atitinkamai lygūs 3 ir 5.
Tuo atveju $c=2$, $r=1$, nes $b_1c=3\cdot 2=6=g$. Skaičių k rasime šitaip:

$$g^1=6^1\equiv 1 \pmod 5\equiv 1 \pmod{b_2}.$$

Taigi $k=r_g(b_2)=1$.
Vadinasi, trupmeną 2/15 skleisdami šešetaine trupmena, gauname begalinę periodinę trupmeną. Periodo ilgis yra 1, priešperiodžio taip pat 1. Atlikę atitinkamus skaičiavimus, gautume

$$\frac{2}{15}=\frac{4}{30}=\frac{1}{6}\cdot\frac{4}{5}=\frac{1}{6}\cdot 0,(4)_{(6)}=0,0(4)_{(6)}.$$

Uždaviniai

17. Trupmenas 2/5, 4/7, 2/9, 5/11, 9/13 užrašykite sisteminėmis trupmenomis pagrindais 5, 6, 8, 9, 12.

18. Raskite periodo ilgius skleisdami sisteminėmis periodinėmis trupmenomis: 2/11 pagrindu 6, 5/6 pagrindu 5, 3/17 pagrindu 12, 5/9 pagrindu 8, $-3/16$ pagrindu 9.

19. Raskite periodo ilgius dešimtaine trupmena skleisdami trupmenas 4/17, 101/23 38/29, 25/31, 41/53, 37/61.

§49. Cikliniai periodo keitimai

Ankstesniame paragrafe įrodėme, kad trupmenos, turinčios tą patį vardiklį, išskleidžiamos vienodo ilgio periodo sisteminėmis periodinėmis trupmenomis. Šiame paragrafe nagrinėsime atvejus, kai ir periodų skaitmenys yra tie patys.

86 teorema. *Jeigu skaičiai* r_1, r_2, ..., r_k, *apibrėžiami* (5.11) *lygybėmis, skaičiai* a *ir* b *tenkina sąlygas*

$$0<a<b,\ (a,\ b)=(b,\ g)=1,$$

tai bet kurios trupmenos r_i/b $(1\leqslant i\leqslant k)$ *periodo skaitmenys gaunami cikliškai keičiant trupmenos* a/b *periodo skaitmenis, t. y.*

$$\frac{r_i}{b}=0,\overline{(c_{i+1}\,c_{i+2}\ldots c_k\,c_1\,c_2\ldots c_i)}_{(g)}.$$

Įrodymas. Pakanka (5.11) lygybes išdėstyti šia tvarka:

$$\begin{aligned}
gr_i &= c_{i+1}b+r_{i+1},\\
gr_{i+1} &= c_{i+2}b+r_{i+2},\\
&\cdots\cdots\cdots\cdots\\
gr_{k-1} &= c_k b+r_k,\\
ga=gr_k &= c_1 b+r_1,\\
&\cdots\cdots\cdots\cdots\\
gr_{i-1} &= c_i b+r_i.
\end{aligned}$$

Čia pasinaudojome 85 teoremoje įrodytu rezultatu, kad $r_k=a$. Iš šių lygybių išplaukia teoremos tvirtinimas, panašiai kaip ir 85 teoremos įrodyme.

87 teorema. *Jeigu* $r_b(g)=\varphi(b)$, *tai visų nesuprastinamų trupmenų* a/b *periodo skaitmenys yra tie patys. Cikliškai keičiant vienos tokios trupmenos periodo skaitmenis, gaunami kitų trupmenų periodai.*

Įrodymas. Visos liekanos r_1, r_2, ..., r_k, apibrėžtos (5.11) lygybėmis, yra skirtingos, nes priešingu atveju periodo ilgis būtų mažesnis už k. Kadangi $(a,b)=(b,g)=1$, tai iš (5.11) lygybių išplaukia $(r_1,b)=(r_2,b)=\ldots=(r_k,b)=1$. Taigi liekanos r_1, r_2, ..., r_k atstovauja visoms liekanų klasėms, tarpusavyje pirminėms su moduliu. Trupmenos, kurių skaitikliai priklauso tai pačiai liekanų klasei moduliu b, turi tuos pačius periodo skaitmenis. Iš tikrųjų, jeigu

$$a\equiv c\,(\mathrm{mod}\,b),$$

$$a=c+bt,$$

tai

$$\frac{a}{b}=\frac{c}{b}+t,$$

t. y. skaičių a/b ir c/b trupmeninės dalys sutampa.

Kadangi skaičiams $r_1, r_2, \ldots, r_k$ teisingas 86 teoremos teiginys, tai jis teisingas visiems skaičiams, tarpusavyje pirminiams su moduliu b, nes šie skaičiai sudaro redukuotąją liekanų sistemą moduliu b.

Teorema įrodyta.

Pavyzdys. Nustatėme, kad trupmeną 15/17 skleisdami dešimtaine trupmena, gausime periodinę trupmeną, kurios periodo ilgis yra $16=\varphi$ (17). Iš tikrųjų

$$\frac{15}{17}=0,(8\ 8\ 2\ 3\ 5\ 2\ 9\ 4\ 1\ 1\ 7\ 6\ 4\ 7\ 0\ 5).$$

Visų kitų trupmenų $a/17$, $(a, 17)=1$, periodų skaitmenys yra tie patys:

$$\frac{14}{17}=0,(8\ 2\ 3\ 5\ 2\ 9\ 4\ 1\ 1\ 7\ 6\ 4\ 7\ 0\ 5\ 8),$$

$$\frac{4}{17}=0,(2\ 3\ 5\ 2\ 9\ 4\ 1\ 1\ 7\ 6\ 4\ 7\ 0\ 5\ 8\ 8),$$

$$\frac{6}{17}=0,(3\ 5\ 2\ 9\ 4\ 1\ 1\ 7\ 6\ 4\ 7\ 0\ 5\ 8\ 8\ 2),$$

$$\frac{9}{17}=0,(5\ 2\ 9\ 4\ 1\ 1\ 7\ 6\ 4\ 7\ 0\ 5\ 8\ 8\ 2\ 3)$$

ir t. t.

Dž. Glesheris (J. Glaisher, 1940, anglų matematikas) nustatė, kad

$$\frac{1}{(g-1)^2}=0,\overline{(0\ 1\ 2\ 3\ldots g-4\ g-3\ g-1)}_{(g)}.$$

Tos trupmenos, užrašytos sistemoje pagrindu g, periodo skaitmenys yra visi neneigiami skaičiai, surašyti iš eilės pradedant 0 ir baigiant $g-1$, trūksta tik skaičiaus $g-2$. Pavyzdžiui,

$$\frac{1}{12^2}=0,(0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ \overline{10}\ \overline{12})_{(13)}.$$

(Brūkšneliai virš 10 ir 12 reiškia, kad tie skaičiai yra vienaženkliai sistemoje pagrindu 13.) Šimtainėje sistemoje trupmena $\frac{1}{99^2}$ užrašoma šitaip:

$$\frac{1}{99^2}=0,(0\ 1\ 2\ 3\ldots\overline{96}\ \overline{97}\ \overline{99})_{(100)}.$$

Buvo bandoma išreikšti sisteminėmis trupmenomis ir iracionaliuosius skaičius. *G. Peano* yra radęs

$$e=10,\ 10110111111000010101000 1\ldots_{(2)},$$

$$\pi=11,\ 00100010000111111011010 10\ldots_{(2)}.$$

Trupmenų a/b skleidimas sisteminėmis trupmenomis paremtas Euklido algoritmu. Yra ir kitokių algoritmų, kuriuos taikant trupmenos a/b išskleidžiamos kitokio tipo begalinėmis eilutėmis. Paminėsime porą tokių algoritmų.

Sakykime, kad

$$g_1, g_2, g_3, \ldots$$

yra begalinė natūrinių skaičių seka, $g_i>1$, x — realusis skaičius.

Apibrėžkime sekas $c_1, c_2, \ldots, x_1, x_2, \ldots$ šitaip:

$$c_0=[x], \quad x_1=x-c_0,$$

$$c_1=g_1 x_1, \quad x_2=g_1 x_1-c_1,$$

$$c_2=g_2 x_2, \quad x_3=g_2 x_2-c_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$c_n=g_n x_n, \quad x_{n+1}=g_n x_n-c_n$$

ir t. t.

Iš šių lygybių gauname

$$x=c_0+\frac{c_1}{g_1}+\frac{c_2}{g_1 g_2}+\frac{c_3}{g_1 g_2 g_3}+\ldots+\frac{c_n}{g_1 g_2 \ldots g_n}+\frac{x_{n+1}}{g_1 g_2 \ldots g_n}.$$

Kai $g_1=g_2=\ldots=g$, taikydami šį algoritmą, gauname skaičiaus x išraišką skaičiaus c_0 ir sisteminės trupmenos pagrindu g suma.

Kai $g_n=n+1$ $(n=1, 2, \ldots)$, gauname skaičiaus x skleidinį trupmenomis, kurių vardikliai – faktorialai:

$$x=c_0+\frac{c_1}{2!}+\frac{c_2}{3!}+\frac{c_3}{4!}+\ldots$$

Įrodyta: kai x yra racionalusis skaičius, taikant šį algoritmą skaičius x išreiškiamas baigtine nurodyto pavidalo dėmenų suma. Kai x yra iracionalusis skaičius, skaičius x išskleidžiamas begaline eilute.

Trumpai aptarsime ir kitą algoritmą.

Sakykime, kad x yra realusis skaičius. Pažymėkime k_1 mažiausią natūrinį skaičių, tenkinantį nelygybę $k_1 x>1$ $(x>0)$. Pažymėję $k_1 x=1+x_1$, matome, kad $x_1>0$. Pažymėkime k_2 mažiausią natūrinį skaičių, su kuriuo $k_2 x_1>1$. Skaičių x_2 apibrėžiame lygybe $k_2 x_1=1+x_2$, jis yra teigiamas. Tęsdami toliau šį procesą, gauname šitokį x skleidinį:

$$x=\frac{1}{k_1}+\frac{1}{k_1 k_2}+\frac{1}{k_1 k_2 k_3}+\ldots;$$

čia visi k_i – natūriniai skaičiai, $k_{n+1}\geqslant k_n$ $(n=1, 2, \ldots)$.

Taikant aptartąjį algoritmą, gautas šis skaičiaus e skleidinys:

$$e=\frac{1}{1}+\frac{1}{1\cdot 1}+\frac{1}{1\cdot 1\cdot 2}+\frac{1}{1\cdot 1\cdot 2\cdot 3}+\ldots$$

Uždaviniai

20. Raskite visų taisyklingų nesuprastinamų trupmenų su vardikliu 23 skleidinius dešimtainėmis periodinėmis trupmenomis.

21. Išskleiskite visas trupmenas $a/11$, $1\leqslant a\leqslant 10$, sisteminėmis trupmenomis pagrindu 7.

Žiedai ir idealai

§50. Žiedas. Žiedo vienetas ir jo dalikliai

Vadovėlio pirmosios dalies 29 paragrafe susipažinome su algebrine struktūra – žiedu. Jį išsamiau nagrinėsime šiame skyriuje. Pirmiausia prisiminsime žiedo apibrėžimą.

Algebrinė struktūra $\check{Z}=(\check{Z}, +, \cdot)$ *su netuščia aibe* $\check{Z}$ *ir dviem vidinėmis binarėmis operacijomis vadinama žiedu, jeigu*:

Ž.1. *Struktūra* $(\check{Z}, +)$ *yra komutatyvioji grupė*;

Ž.2. $(\forall a, b, c \in \check{Z})\ (ab)c=a(bc)$;

Ž.3. $(\forall a, b, c \in \check{Z})$ 1) $(a+b)c=ac+bc$,
2) $c(a+b)=ca+cb$.

Jeigu dar ir

Ž.4. $(\forall a, b \in \check{Z})\ ab=ba$,

tai žiedas $\check{Z}$ *vadinamas komutatyviuoju.*

Jeigu $\check{Z}$ *yra baigtinė aibė, tai žiedas vadinamas baigtiniu žiedu.*

Žiedo operacija „+“ vadinama sudėtimi, o „·“ – daugyba. *Grupė* $(\check{Z}, +)$ *vadinama žiedo* $\check{Z}$ *adicine grupe.* Prisiminę komutatyviosios grupės apibrėžimą, galime konstatuoti, kad teiginys Ž. 1 ekvivalentus šitokių teiginių konjunkcijai:

Ž.1.1. $(\forall a, b, c \in \check{Z})\ (a+b)+c=a+(b+c)$,

Ž.1.2. $(\exists O \in \check{Z})\ (\forall a \in \check{Z})\ a+O=O+a=a$,

Ž.1.3. $(\forall a \in \check{Z})\ (\exists -a \in \check{Z})\ a+(-a)=(-a)+a=0$,

Ž.1.4. $(\forall a, b \in \check{Z})\ a+b=b+a$.

Žiedo aksiomų pavadinimai žinomi iš vadovėlio pirmosios dalies 29 paragrafo. Tik pažymėsime, kad sudėties neutralusis elementas O, kurio egzistavimą garantuoja Ž. 1. 2 ir kurio vienatis išplaukia iš grupių 2 savybės (§ 27), vadinamas žiedo $\check{Z}$ nuliu. Jį visada žymėsime O, ir tik ten, kur galima supainioti jį su kito žiedo nuliu, prirašysime indeksą ar numerį. Žiedų paprasčiausios bendrosios savybės išnagrinėtos vadovėlio 1 dalies 29 paragrafe, todėl toliau jas laikysime žinomomis.

Iš žiedo apibrėžimo neišplaukia, kad egzistuoja daugybos neutralusis elementas. Tačiau (žr. 1 d., § 29, žiedo daugybos savybes) jeigu toks elementas egzistuoja, tai jis yra vienintelis.

Žiedo $\check{Z}$ daugybos neutralųjį elementą, kai jis egzistuoja, vadiname *žiedo* $\check{Z}$ *vienetu.*

Žiedo vienetą žymėsime raide e. Tuo atveju, kai galima supainioti kelių žiedų vienetus, juos numeruosime arba prirašysime indeksus. Konkrečių žiedų vienetai bus konkretūs objektai.

Vadovėlio 1 dalyje aptarėme nemažai žiedų. Priminsime keletą iš jų.

1. Sveikųjų skaičių žiedas ($\mathbf{Z}$, $+$, $\cdot$) yra komutatyvusis žiedas su vienetu.

2. Sveikųjų skaičiaus m kartotinių aibė $\mathbf{Z}_m$ su sudėtimi ir daugyba — komutatyvusis žiedas; be vieneto, kai $m \neq \pm 1$.

3. n-osios eilės kvadratinių matricų su elementais iš lauko $\mathbf{L}$ žiedas $\mathfrak{M}_n(\mathbf{L})$ — nekomutatyvusis žiedas su vienetu E_n; čia $n=2, 3, \ldots$ Taigi tokių žiedų yra be galo daug (1 d., § 60, 73 teorema).

4. n-matės vektorinės erdvės tiesinių operatorių aibė su sudėtimi ir daugyba — nekomutatyvusis žiedas su vienetu (1 d., § 83). Aišku, kad tokių žiedų yra tiek, kiek yra n-mačių, $n=2, 3, \ldots$, vektorinių erdvių.

5. 28 paragrafe susipažinome su liekanų klasių moduliu m ($m \in \mathbf{N}$) žiedais. Tai baigtiniai komutatyvieji žiedai su vienetais. Jų yra tiek, kiek yra natūrinių skaičių m, didesnių už 1.

Žiedo su vienetu bazinės aibės elementas gali turėti atvirkštinį (simetrišką daugybos atžvilgiu) elementą arba jo neturėti. Iš pirmosios dalies 29 paragrafo žinome: *jeigu elementas a turi atvirkštinį elementą a^{-1}, tai tiktai vieną.*

Pavyzdžiui, n-osios eilės kvadratinių matricų žiede atvirkštinius elementus turi tik reguliariosios matricos, o liekanų klasių mod m žiede $\mathbf{L}_m$ atvirkštinius elementus turi tik tos liekanų klasės K_r, kurių $D(r, m)=1$.

Žiedo $\check{\mathbf{Z}}$ su vienetu bazinės aibės $\check{Z}$ elementas a, turintis atvirkštinį, vadinamas vieneto dalikliu.

88 teorema. *Žiedo $\check{\mathbf{Z}}$ vieneto daliklių aibė yra multiplikacinė grupė. Jeigu žiedas komutatyvus, tai ir ta grupė komutatyvi.*

Įrodymas. Kaip žinome iš vadovėlio 1 dalies 29 paragrafo, jeigu a ir b turi atvirkštinius elementus, tai $(ab)^{-1}=b^{-1}a^{-1}$. Taigi žiedo $\check{\mathbf{Z}}$ vieneto daliklių aibė uždara daugybos atžvilgiu. Vieneto daliklių daugybos asociatyvumas (atitinkamai komutatyvumas) išplaukia iš žiedo $\check{\mathbf{Z}}$ daugybos asociatyvumo (komutatyvumo). Žinome, kad $e^{-1}=e$ ir $(a^{-1})^{-1}=a$. Taigi vieneto daliklių aibei priklauso vienetas e, o vieneto dalikliui atvirkštinis elementas irgi yra vieneto daliklis.

Žiede su vienetu galima apibrėžti ekvivalentumo sąryšį.

Žiedo su vienetu $\check{\mathbf{Z}}$ elementas b vadinamas asocijuotu elementui a, jeigu yra toks vieneto daliklis ε, su kuriuo teisinga lygybė $b=\varepsilon a$. Rašoma $b \sim a$.

89 teorema. *Sąryšis „b asocijuotas a“ yra ekvivalentumo sąryšis aibėje $\check{Z}$.*

Įrodymas. Kadangi $a=ea$, tai $a\sim a$. Lygybę $b=\varepsilon a$ padauginę iš kairės iš ε^{-1}, gauname $a=\varepsilon^{-1}b$. Tada, jeigu $b\sim a$, tai ir $a\sim b$. Jeigu $b\sim a$ ir $c\sim b$, tai $b=\varepsilon_1 a$, $c=\varepsilon_2 b$ ir $c=(\varepsilon_1\varepsilon_2)a=\varepsilon a$. Todėl $c\sim a$.

Pagal sąryšį „*b asocijuotas a*" aibė $\check{Z}$ gali būti suskaidyta į ekvivalentumo klases.

Aibė $K_a=\{b \mid b\sim a\}$ *– ekvivalentumo klasė sąryšio* $\sim$ *atžvilgiu.*

Pavyzdžiai. 1. Gauso sveikųjų skaičių žiedas

$$\mathbf{Z}[i]=(\{m+in \mid m,\ n\in\mathbf{Z}\},\ +,\ .)$$

turi vieneto daliklius 1, -1, i, $-i$. Todėl su kiekvienu $m+in\in\mathbf{Z}[i]$

$$K_{m+in}=\{m+in,\ -m-in,\ -n+im,\ n-im\}.$$

2. Sveikųjų skaičių žiedo **Z** vieneto dalikliai yra 1 ir -1. Todėl

$$(\forall\, m\in\mathbf{Z})\ K_m=\{m,\ -m\}.$$

3. n-osios eilės kvadratinių matricų virš lauko **L** žiede vieneto dalikliai yra reguliariosios matricos. Todėl

$$\left(\forall\, B\in\mathfrak{M}_n(\mathbf{L})\right)\quad K_B=\{AB \mid |A|\neq 0\}.$$

Akivaizdus šitoks teiginys: *jeigu komutatyviojo žiedo su vienetu kiekvienas nenulinis elementas turi atvirkštinį, tai tas žiedas yra laukas.* Šiuo požymiu galima remtis tikrinant, ar žiedas yra laukas.

Žiedo $\check{\mathbf{Z}}$ *su vienetu e charakteristika vadinamas mažiausias natūrinis skaičius m, su kuriuo*

$$me=0.$$

Jeigu tokio skaičiaus m nėra, tai žiedas vadinamas nulinės charakteristikos žiedu.

Primename, kad $me=\underbrace{e+e+\ldots+e}_{m\ \text{dėmenų}}$.

Kiekvienas baigtinis žiedas yra nenulinės charakteristikos. Iš tikrųjų, tarus, kad tokio žiedo charakteristika lygi 0, išplauktų, jog jo vieneto kartotiniai me yra skirtingi ir tų kartotinių yra be galo daug.

Pavyzdžiui, žiedo L_m charakteristika lygi m, nes $mK_1=K_m=K_0$, o $l\cdot K_1=K_l\neq K_0$, kai $l<m$.

Žiedo $\check{\mathbf{Z}}=(\check{Z},\ +,\ \cdot)$ *požiedžiu vadinamas žiedas* $\check{\mathbf{Z}}_1=(\check{Z}_1,\ +,\ \cdot)$, $\check{Z}_1\subseteq\check{Z}$.

Ar kuris nors poaibis yra požiedis, galima įsitikinti remiantis šitokia teorema.

90 teorema. *Sakykime* $\check{Z}=(\check{Z}, +, \cdot)$ *yra žiedas ir* $\check{Z}_1 \subset \check{Z}$. $\check{Z}_1=(\check{Z}_1, +, \cdot)$ *yra žiedo* $\check{Z}$ *požiedis tada ir tik tada, kai*

$$(\forall a,\ b \in \check{Z}_1)\ a-b \in \check{Z}_1,\ ab \in \check{Z}_1.$$

Įrodymas. Būtinumas. Jeigu $\check{Z}_1$ yra žiedo $\check{Z}$ požiedis, tai $(\forall a, b \in \check{Z}_1)$ $a-b \in \check{Z}_1$ (1d., § 29) ir $ab \in \check{Z}_1$. Taigi teoremos sąlygos būtinos.

Pakankamumas. Tarkime, kad teoremos sąlygos išpildytos. Įsitikinsime, kad aibėje $\check{Z}_1$ galima sudėtis. Turime $(\forall a, b \in \check{Z}_1)$ $a-a=O \in \check{Z}_1$, o $O-b=-b \in \check{Z}_1$, $a-(-b)=a+b \in \check{Z}_1$.

Kartu įrodėme, kad $O \in \check{Z}_1$ ir $(\forall b \in \check{Z}_1)$ $-b \in \check{Z}_1$. Visos kitos žiedo apibrėžimo sudėties ir daugybos savybės yra ir aibėje $\check{Z}_1$, nes jos yra aibėje $\check{Z}$, o $\check{Z}_1 \subset \check{Z}$. Taigi teoremos sąlygos pakankamos.

91 teorema. *Žiedo* $\check{Z}$ *su vienetu e poaibis* $\{me \mid m \in \mathbf{Z}\}$ *yra žiedo* $\check{Z}$ *požiedis. Tas požiedis izomorfiškas sveikųjų skaičių žiedui* $\mathbf{Z}$, *kai žiedo* $\check{Z}$ *charakteristika lygi nuliui, ir liekanų klasių moduliu m žiedui* $\mathbf{L}_m$, *kai žiedo* $\check{Z}$ *charakteristika lygi m.*

Įrodymas. 1. Patikrinsime, ar aibė $\{me \mid m \in \mathbf{Z}\}$ tenkina 90 teoremos sąlygas. Kadangi iš $m, k \in \mathbf{Z}$ išplaukia $me-ke=(m-k)e$ ir $(me)(ke)=(mk)e$, o $m-k \in \mathbf{Z}$ ir $mk \in \mathbf{Z}$, tai 90 teoremos sąlygos tenkinamos. Ta aibė yra žiedo $\check{Z}$ požiedis.

2. Kai žiedo $\check{Z}$ charakteristika lygi 0, bijekcija

$$\varphi\colon \{me \mid m \in \mathbf{Z}\} \leftrightarrow \mathbf{Z},$$

apibrėžta lygybe $\varphi(me)=m$, yra izomorfizmas, nes

$$\varphi(me+ke)=\varphi\big((m+k)e\big)=m+k=\varphi(me)+\varphi(ke)$$

ir

$$\varphi(me \cdot ke)=\varphi\big((mk)e\big)=mk=\varphi(me)\cdot\varphi(ke).$$

3. Kai žiedo $\check{Z}$ charakteristika lygi m,

$$\{ke \mid k \in \mathbf{Z}\}=\{0,\ e,\ 2e,\ \ldots,\ (m-1)e\}.$$

Tuo atveju bijekcija $\varphi(ke)=K_k$, $k=0, 1, \ldots, m-1$, irgi yra izomorfizmas.

Pavyzdys. n-osios eilės kvadratinių matricų su sveikaisiais elementais aibė $\mathfrak{M}_n(\mathbf{Z})$ yra n-osios eilės kvadratinių matricų su realiaisiais elementais žiedo aibės poaibis.

Kadangi $A=(a_{ij})$, $B=(b_{ij})$ ir $a_{ij}, b_{ji} \in \mathbf{Z}$, tai

$$A-B=(a_{ij}-b_{ij}),\ AB=(c_{ij}),\ c_{ij}=\sum_{k=1}^{n} a_{ik}b_{kj};$$

čia $a_{ij}-b_{ij}$, c_{ij} – sveikieji skaičiai.

Taigi matricų su sveikaisiais elementais aibė $\mathfrak{M}_n(\mathbf{Z})$ yra žiedo $\mathfrak{M}_n(\mathbf{R})$ požiedis.

Uždaviniai

1. Įrodykite, kad šios skaičių aibės su sudėtimi ir daugyba yra žiedai:

1) $\mathbf{Z}[\sqrt[3]{k}]=\{m+n\sqrt[3]{k} \mid m, n\in\mathbf{Z}\}$, $k\in\mathbf{N}$;

2) $\mathbf{Z}[\sqrt[3]{k}]=\{m+n\sqrt[3]{k}+l\sqrt[3]{k^2} \mid m, n, l\in\mathbf{Z}\}$, $k\in\mathbf{N}$;

3) $\mathbf{Z}[i]=\{m+in \mid m, n\in\mathbf{Z}\}$; čia $i^2=-1$.

2. Patikrinkite, ar struktūra $(\mathbf{Z}^2, +, \cdot)$, kai sudėtis ir daugyba apibrėžtos formulėmis

$$(m, n)+(k, l)=(m+k, n+l),\ (m, n)\cdot(k, l)=(mk, nl),$$

yra žiedas. Raskite to žiedo nulį, vienetą, vieneto daliklius, ekvivalentumo klases sąryšio „asocijuoti" atžvilgiu.

3. Įrodykite, kad žiedas $\mathbf{Z}[\sqrt{2}]$ turi be galo daug vieneto daliklių. Raskite kelis iš jų. Patikrinkite, ar šios struktūros yra žiedai. Raskite jų visus arba kelis vieneto daliklius.

4. $\left(\left\{\begin{pmatrix} m & n \\ -n & m \end{pmatrix} \mid m, n\in\mathbf{Z}\right\}, +, \cdot\right)$.

5. $\left(\left\{\begin{pmatrix} m & n \\ -2n & m \end{pmatrix} \mid m, n\in\mathbf{Z}\right\}, +, \cdot\right)$.

6. $\left(\left\{\begin{pmatrix} m_1 & 0 & \dots & 0 \\ 0 & m_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & m_n \end{pmatrix} \mid m_j\in\mathbf{Z},\ j=1, \dots, n\right\}, +, \cdot\right)$;

čia $n\geqslant 2$, $n\in\mathbf{N}$.

7. Raskite žiedo $\mathbf{L}_{24}$ vieneto daliklius ir asocijuotų elementų klases.

§51. Integralumo sritis. Dalumo sąryšis integralumo srityje

Yra žiedų, pasižyminčių „keistomis" savybėmis. Juose dviejų nelygių nuliui elementų sandauga gali būti lygi nuliui. Pavyzdžiui, liekanų klasių moduliu 20 žiede $\mathbf{L}_{20}$ $K_4\cdot K_{15}=K_0$, $K_2\cdot K_{10}=K_0$, o $K_0=O_{L_{20}}$. Panašiai antrosios eilės kvadratinių matricų žiede

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

nors daugikliai nėra nuliai.

Žiedo $\mathbf{Ž}$ *nenuliniai elementai* a *ir* b, *su kuriais*

$$ab=0,$$

vadinami nulio dalikliais.

Pateiktieji pavyzdžiai rodo, kad kai kurie liekanų klasių žiedai, matricų žiedai turi nulio daliklių. Yra ir daugiau tokių žiedų.

Komutatyvusis žiedas, neturintis nulio daliklių, vadinamas integralumo sritimi.

Nesunku įsitikinti, kad kiekvienas skaičių žiedas, ar jis būtų sveikųjų skaičių žiedo **Z** požiedis, ar plėtinys, neturi nulio daliklių – yra integralumo sritis. $\mathbf{L}_p$, kai p – pirminis skaičius, irgi yra integralumo sritis – laukas (52 teorema).

Kiekvienas laukas yra integralumo sritis. Tačiau ne kiekviena integralumo sritis yra laukas. Pavyzdžiui, sveikųjų skaičių žiedas nėra laukas.

92 teorema. *Kiekviena baigtinė integralumo sritis su vienetu yra laukas.*

Įrodymas. Sakykime, $\check{\mathbf{Z}}$ – integralumo sritis ir $\check{Z}=\{a_1, \ldots, a_n\}$. Norint įsitikinti, kad $\check{\mathbf{Z}}$ yra laukas, užtenka įrodyti, jog kiekvienas nelygus nuliui elementas turi atvirkštinį. Tegul $a_1=O$ ir $a_2=e$. Išnagrinėkime sandaugas

$$a_i a_1, \; a_i a_2, \; \ldots, \; a_i a_n,$$

kai $a_i \neq O$. Tarp šių sandaugų nėra lygių, nes tarus, kad $a_i a_j = a_i a_k$, kai $k \neq j$, išplauktų $a_i (a_j - a_k) = O$ ir $a_i \neq O$, $a_j - a_k \neq 0$. Tai reikštų, kad žiede $\check{\mathbf{Z}}$ yra nulio daliklių. Todėl su tam tikru j bus $a_i a_j = e$. Pastaroji lygybė reiškia, kad $(a_i)^{-1} = a_j$.

Išvada. *Integralumo srities su vienetu charakteristika yra arba nulis, arba pirminis skaičius.*

93 teorema. *Netrivialus komutatyvusis žiedas yra integralumo sritis tada ir tik tada, kai daugyba turi prastinimo iš kiekvieno nenulinio elemento savybę.*

Įrodymas. Būtinumas. Jeigu $\check{\mathbf{Z}}$ yra integralumo sritis, tai iš $ab=O$ gauname $(a=O) \vee (b=O)$. Jeigu $ab=ac$ ir $a \neq O$, tai $ab-ac=a(b-c)=O$ ir $b-c=O$, t. y. $b=c$.

Pakankamumas. Tarkime, kad iš lygybės $ab=ac$, kai $a \neq O$, išplaukia $b=c$. Tada su kiekvienu $a \neq O$ iš $ab=O$ gausime $ab=aO$, $a(b-O)=O$. Taigi $b=O$. Pastaroji lygybė reiškia, kad žiede nėra nulio daliklių.

Integralumo srityje su vienetu, kaip ir sveikųjų skaičių aibėje, galima apibrėžti dalumo sąryšį.

Tarkime, kad $\check{\mathbf{Z}}$ – integralumo sritis su vienetu e.

Sakoma, kad $a \in \check{Z}$ dalijasi iš nelygaus nuliui $\check{\mathbf{Z}}$ elemento b, jeigu yra toks $q \in \check{Z}$, su kuriuo $a=bq$. Rašoma $b|a$. Elementas b vadinamas elemento a dalikliu. Elementas a vadinamas elemento b kartotiniu. Daliklis q vadinamas elementų a ir b santykiu.

94 teorema. *Jeigu integralumo srityje* $b|a$, *tai santykis* q $(a=bq)$ *randamas vienareikšmiškai.*

Įrodymas. Tarkime, kad $a=bq$ ir $a=bq_1$. Tada turėsime lygybę $O=b\,(q-q_1)$, iš kurios išplaukia $q-q_1=O$ ir $q=q_1$, nes $b\neq O$.

Pavyzdžiui, žiede $\mathbf{L}_{13}$ $K_5|K_2$, nes $K_2=K_5\cdot K_3$.
Gauso sveikųjų skaičių žiede $\mathbf{Z}$ $[i]$ skaičius $27+11i$ dalijasi iš $3+4i$, nes $(3+4i)(5-3i)=27+11i$. $5+7i$ nesidalija iš $4+i$.

Integralumo srityje su vienetu dalumo sąryšio savybės analogiškos sveikųjų skaičių žiedo dalumo sąryšio savybėms. Jos ir įrodomos analogiškai.

Dalumo sąryšio integralumo srityje savybės.

1. *Kiekvienas elementas dalijasi iš vieneto kiekvieno daliklio.*

Įrodymas. Jeigu ε – vieneto daliklis, tai $e=\varepsilon\varepsilon^{-1}$ ir $a=ea=\varepsilon\,(\varepsilon^{-1}a)$.

2. *Jeigu* $a\neq O$ *ir* ε *– bet koks vieneto daliklis, tai* $\varepsilon a|a$ *ir* $a|\varepsilon a$.

Įrodymas. Jeigu ε – vieneto daliklis, tai $a=ea=\varepsilon^{-1}(\varepsilon a)$.

3. *Integralumo srities nulinis elementas* O *dalijasi iš kiekvieno nelygaus nuliui tos srities elemento.*

Įrodymas. $O=a\cdot O$.

4. *Jeigu* $b|a$, *tai su kiekvienu vieneto dalikliu* ε $\varepsilon b|a$.

Įrodymas. Jeigu $b|a$, tai $a=bq$. Tada $a=(\varepsilon b)\,(\varepsilon^{-1}q)$.

5. *Jeigu* $b|a$ *ir* $c|b$, *tai* $c|a$.

Įrodymas. Jeigu $b|a$ ir $c|b$, tai $a=bq_1$ ir $b=cq_2$. Tada $a=cq_2q_1=c\,(q_1q_2)$.

6. *Jeigu* $b|a$, *tai su kiekvienu* $d\neq O$, $bd|ad$.

Įrodymas. Kadangi $b\neq O$ ir $d\neq O$, tai $bd\neq O$. Jeigu $b|a$, tai $a=bq$. Tada $ad=bqd=(bd)q$.

7. *Jeigu* $b|a$, *tai su kiekvienu* d $b|ad$.

Įrodymas. Iš lygybės $a=bq$ gauname $ad=(bq)d=b(dq)$.

8. *Jeigu* $b|a_i$, $i=1, 2, \ldots, n$, *tai su bet kokiais integralumo srities elementais* $c_1, c_2, \ldots, c_n$

$$b \mid \sum_{i=1}^{n} c_i a_i.$$

Įrodymas. Jeigu $b|a_i$, tai $a_i=bq_i$, $q_i\in\check{Z}$, $i=1, 2, \ldots, n$. Tada $c_ia_i=c_ibq_i=b(c_iq_i)$ ir

$$\sum_{i=1}^{n} c_i a_i = b \sum_{i=1}^{n} c_i q_i.$$

Paėmę šioje savybėje $n=2$, $c_1=e$, $c_2=e$, $c_1=e$, $c_2=-e$, gauname **išvadą:** *jeigu elementai a ir c dalijasi iš b, tai jų suma $a+c$ ir skirtumas $a-c$ dalijasi iš b.*

9. *Jeigu $b|a$ ir $d|c$, tai $bd|ac$.*

Įrodymas. Sudauginę lygybes $a=bq_1$ ir $c=bq_2$, gauname

$$ac=(bd)(q_1q_2).$$

10. *Jeigu $b|a$, tai su bet kokiu natūriniu n $b^n|a^n$.*

Įrodymas. Jeigu $a=bq$, tai $a^n=(bq)^n=b^nq^n$.

11. *Jeigu $b|a$ ir $a|b$,* tai $a\sim b$ (asocijuoti).

Įrodymas. Kadangi $b|a$ ir $a|b$, tai $a=bq_1$, $b=aq_2$. Todėl $a=aq_2q_1$ ir $q_1q_2=e$. Taigi q_1 – vieneto daliklis, ir $a\sim b$.

Atkreipsime dėmesį, kad dalumo sąvoką galima apibrėžti ir kiekviename komutatyviajame žiede. Bet tada negalima būtų įrodyti 94 teoremos. Taip pat nebūtų teisingos ir dauguma iš 1–11 savybių.

Kaip įsitikinome, kiekvienas integralumo srities su vienetu nenulinis elementas *a* dalijasi iš vieneto ir vieneto daliklių, taip pat iš kiekvieno sau asocijuoto elemento *b*. *Tuos daliklius vadiname trivialiaisiais.*

Elemento $a\neq O$ daliklis c, kuris nėra nei vieneto daliklis, nei elementui a asocijuotas elementas, vadinamas tiesioginiu dalikliu.

Remdamiesi dalumo sąryšiu ir pastaraja sąvoka, visą integralumo srities aibę galime suskaidyti į keturias aibes:

$\check{Z}=\{O\}\cup\check{Z}_v\cup\check{Z}_p\cup\check{Z}_s$,

$\check{Z}_v$ – vieneto daliklių aibę,

$\check{Z}_p$ – aibę nenulinių elementų, kurie nėra vieneto dalikliai ir neturi tiesioginių daliklių,

$\check{Z}_s$ – aibę nenulinių elementų, kurie turi tiesioginių daliklių.

Integralumo srities su vienetu nenulinis elementas, kuris nėra vieneto daliklis ir neturi tiesioginių daliklių, vadinamas pirminiu elementu. Nenulinis elementas, turintis tiesioginių daliklių, vadinamas sudėtiniu.

Kyla klausimas, ar integralumo srityje teisingi teiginiai apie pirminius ir sudėtinius elementus, analogiški atitinkamiems teiginiams sveikųjų skaičių žiede. Į tai mėginsime atskyti kituose paragrafuose, pasitelkdami idealų teorijos elementus.

Uždaviniai

8. Patikrinkite, ar 2 uždavinio žiedas yra integralumo sritis.

9. Įrodykite šiuos teiginius:

a) jeigu komutatyviojo žiedo $\check{\mathbf{Z}}$ elementai a ir b yra nulio dalikliai, tai su kiekvienais $c \neq O$ ir $d \neq O$ žiedo $\check{\mathbf{Z}}$ elementais ac ir bd yra nulio dalikliai;

b) žiedo su vienetu nulio daliklis neturi atvirkštinio elemento.

10. Raskite 2 uždavinio žiedo nulio daliklius.

11. Patikrinkite, ar žiede $\mathbf{Z}[\sqrt{2}]$:

a) $5-17\sqrt{2}$ dalijasi iš $5+\sqrt{2}$;

b) $6-7\sqrt{2}$ dalijasi iš $3-2\sqrt{2}$;

c) $58+\sqrt{2}$ dalijasi iš $3+5\sqrt{2}$.

12. Patikrinkite, ar žiede $\mathbf{Z}[\sqrt{3}]$:

a) $3+2\sqrt{3}$ dalijasi iš $2+\sqrt{3}$;

b) $54-7\sqrt{3}$ dalijasi iš $3-4\sqrt{3}$;

c) $6+5\sqrt{3}$ dalijasi iš $2+3\sqrt{3}$.

13. Patikrinkite, ar Gauso sveikųjų skaičių žiede $\mathbf{Z}[i]$:

a) $4+8i$ dalijasi iš $3+i$;

b) $8-15i$ dalijasi iš $4-3i$;

c) $43-15i$ dalijasi iš $6+5i$.

§52. Komutatyviųjų žiedų idealai

Šiame ir kituose šio skyriaus paragrafuose nagrinėjami tik komutatyvieji žiedai. Todėl toliau, kad būtų trumpiau, vietoj „komutatyvusis žiedas“ rašysime tiesiog „žiedas“.

Nagrinėjant dalumą žieduose, taip pat žiedų homomorfizmus, vartojama žiedo idealo sąvoka. Remiantis šia sąvoka, pavyksta išskirti tokius žiedus, kurie į skaičių žiedus labiau panašūs negu integralumo sritys su vienetu.

Žiedo $\check{\mathbf{Z}}=(\check{Z}, +, \cdot)$ *netuščias poaibis* $\mathfrak{A}$ *vadinamas žiedo* $\check{\mathbf{Z}}$ *idealu, jeigu*:

I.1. $(\forall a,\ b \in \mathfrak{A})\ a-b \in \mathfrak{A}$,

I.2. $(\forall a \in \mathfrak{A},\ z \in \check{\mathbf{Z}})\ az \in \mathfrak{A}$.

Kiekvienas (komutatyvusis) žiedas turi idealus $\{O\}$ ir $\check{\mathbf{Z}}$, kurie vadinami atitinkamai *nuliniu* ir *vienetiniu* idealais. Be šių idealų, žiede galima sukonstruoti idealus remiantis šitokia teorema.

95 teorema. *Jeigu* $a_1, a_2, \ldots, a_n,\ n \in \mathbf{N}$, *yra bet kokie žiedo* $\check{\mathbf{Z}}=(\check{Z}, +, \cdot)$ *elementai, tai aibė* $\mathfrak{A}=\left\{\sum_{j=1}^{n} x_j a_j \mid x_j \in \check{Z},\ j=1, 2, \ldots, n\right\}$ *yra idealas.*

Įrodymas. Jeigu $a,\ b \in \mathfrak{A}$, tai

$$a = \sum_{j=1}^{n} t_j a_j, \quad b = \sum_{j=1}^{n} u_j a_j, \quad t_j,\ u_j \in \check{Z}, \quad j = 1, \ldots, n.$$

Tada

$$a - b = \sum_{j=1}^{n} (t_j - u_j) a_j \in \mathfrak{A}, \quad \text{nes} \quad t_j - u_j \in \check{Z}, \quad j = 1, \ldots, n.$$

Taigi I. 1 savybė yra.

Kadangi su kiekvienu $z \in \check{Z}$ ir su kiekvienu $a \in \mathfrak{A}$

$$az = \sum_{j=1}^{n} (t_j z) a_j \in \mathfrak{A},$$

nes $t_j z \in \check{Z}$, tai ir 1.2 savybė yra.

Idealą $\left\{ \sum_{j=1}^{n} x_j a_j \mid x_j \in \check{Z}, \quad j = 1, \ldots, n \right\}$ *vadiname idealu, generuotu elementų* $a_1, a_2, \ldots, a_n$, *ir žymime* $(a_1, a_2, \ldots, a_n)$.

Idealas (a), *generuotas vieno elemento* a, *vadinamas vyriausiuoju idealu*:

$$(a) = \{ za \mid z \in \check{Z} \}.$$

Pavyzdžiui, aibė $\mathbf{Z}_m = \{mt \mid t \in \mathbf{Z}\}$ yra sveikųjų skaičių žiedo $\mathbf{Z}$ vyriausiasis idealas su kiekvienu natūriniu m. Kai $m = 1$, toji aibė lygi $\mathbf{Z}$, o kai $m > 1$, ji yra skaičiaus m kartotinių aibė. Anksčiau nustatėme, kad ta aibė yra modulis.

96 teorema. 1. *Žiedo* $\check{Z}$ *kiekvienas idealas* $\mathfrak{A}$ *yra to žiedo požiedis.* 2. *Žiedo* $\check{Z}$ *kiekvienas požiedis, uždaras jo elementų daugybos iš žiedo elementų atžvilgiu, yra idealas.*

Įrodymas. 1. Jeigu $\mathfrak{A}$ yra idealas, tai I. 1 savybė ir iš I. 2 išplaukianti savybė $(\forall a,\ b \in \mathfrak{A})\ ab \in \mathfrak{A}$ yra 90 teoremos sąlygos. Taigi $\mathfrak{A}$ – požiedis. 2. Jeigu $\mathfrak{A}$ yra žiedo $\check{Z}$ požiedis, uždaras jo elementų daugybos iš žiedo elementų atžvilgiu, tai aibėje $\mathfrak{A}$ teisinga I. 2 savybė. I. 1 savybė išplaukia iš 90 teoremos.

97 teorema. *Jeigu žiedo* $\check{Z}$ *su vienetu vienetinis elementas* e *priklauso idealui* $\mathfrak{A}$, *tai* $\mathfrak{A} = \check{Z}$.

Įrodymas. $\mathfrak{A} \subset \check{Z}$. Iš I. 2 išplaukia $(\forall z \in \check{Z})\ ez = z \in \mathfrak{A}$. Tai reiškia, kad $\check{Z} \subset \mathfrak{A}$. Taigi $\mathfrak{A} = \check{Z}$.

98 teorema. *Kiekvienas laukas turi tik du idealus – nulinį ir vienetinį.*

Įrodymas. Jeigu $\mathfrak{A}$ – lauko **L** idealas ir $\mathfrak{A} \neq (O)$, tai yra toks $a \neq O$, kad $a \in \mathfrak{A}$. Kadangi $a^{-1} \in L$, tai pagal I. 2 $aa^{-1} = e \in \mathfrak{A}$. Taigi $\mathfrak{A} = L$.

99 teorema. *Žiedo idealų sankirta yra to paties žiedo idealas.*

Įrodymas. Jeigu $\mathfrak{A}_1$ ir $\mathfrak{A}_2$ yra žiedo $\check{Z}$ idealai ir $\mathfrak{A} = \mathfrak{A}_1 \cap \mathfrak{A}_2$, tai su kiekviena pora a, $b \in \mathfrak{A}$

$$a \in \mathfrak{A}_1,\ a \in \mathfrak{A}_2 \text{ ir } b \in \mathfrak{A}_1,\ b \in \mathfrak{A}_2.$$

Tada pagal I. 1 $a - b \in \mathfrak{A}_1$ ir $a - b \in \mathfrak{A}_2$, taigi ir $a - b \in \mathfrak{A}$. Pagal I.2 $az \in \mathfrak{A}_1$ ir $az \in \mathfrak{A}_2$, taigi ir $az \in \mathfrak{A}$ su kiekvienu $z \in \check{Z}$.

Analogiškai samprotaudami, įrodysime teoremą ir daugiau kaip dviejų idealų sankirtai.

Žiedo $\check{Z}$ idealų $\mathfrak{A}_1$ ir $\mathfrak{A}_2$ suma vadiname aibę

$$\mathfrak{A}_1 + \mathfrak{A}_2 = \{ x + y \mid x \in \mathfrak{A}_1,\ y \in \mathfrak{A}_2 \}.$$

100 teorema. *Žiedo dviejų idealų suma yra to žiedo idealas.*

Įrodymas. Jeigu a, $b \in \mathfrak{A}_1 + \mathfrak{A}_2$, tai $a = x_1 + y_1$, $b = x_2 + y_2$, x_1, $x_2 \in \mathfrak{A}_1$, y_1, $y_2 \in \mathfrak{A}_2$. Tada $a - b = (x_1 - x_2) + (y_1 - y_2)$ yra aibės $\mathfrak{A}_1 + \mathfrak{A}_2$ elementas, nes $x_1 - x_2 \in \mathfrak{A}_1$, $y_1 - y_2 \in \mathfrak{A}_2$ pagal I. 1. Su bet kuriuo $z \in \check{Z}$ $az = (x_1 + y_1)z = x_1 z + y_1 z$ irgi yra aibės $\mathfrak{A}_1 + \mathfrak{A}_2$ elementas, nes $x_1 z \in \mathfrak{A}_1$ ir $y_1 z \in \mathfrak{A}_2$ pagal I. 2.

Idealų $\mathfrak{A}_i$, $i = 1, 2, \ldots, n$, suma vadinama aibė

$$\mathfrak{A}_1 + \ldots + \mathfrak{A}_n = \left\{ \sum_{i=1}^{n} x_i \mid x_i \in \mathfrak{A}_i,\quad i = 1, \ldots, n \right\}.$$

Teisingas šitoks teiginys – 100 teoremos apibendrinimas: *žiedo $\check{Z}$ idealų $\mathfrak{A}_1$, $\mathfrak{A}_2$, ..., $\mathfrak{A}_n$ suma yra to žiedo idealas.*

Įrodyti paliekame skaitytojui.

Pavyzdžiai. 1. Jeigu a_1, ..., a_n yra žiedo elementai, tai $(a_i) = \{xa_i \mid x \in \check{Z}\}$, $i = 1, \ldots, n$, o

$$(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} x_i a_i \mid x_i \in \check{Z} \right\} = \left\{ \sum_{i=1}^{n} z_i \mid z_i \in \mathfrak{A}_i \right\} = (a_1) + \ldots + (a_n).$$

2. Sveikųjų skaičių žiede **Z** turime $(3, 5) = (3) + (5)$ arba $(4, 3, 6) = (4) + (3) + (6)$.

§53. Lyginiai pagal idealą. Žiedo faktoržiedas

Kiekviename (komutatyviajame) žiede $\check{Z}$ galima apibrėžti sąryšį, analogišką sveikųjų skaičių žiedo sąryšiui „*lygsta* mod m“.

Tarkime, kad $\check{Z}=(\check{Z}, +, \cdot)$ yra žiedas, o $\mathfrak{A}$ – jo idealas, $a, b\in\check{Z}$.

Sakoma, kad a lygsta b pagal idealą $\mathfrak{A}$ (arba a kongruentus b moduliu $\mathfrak{A}$), *ir rašoma* $a\equiv b \pmod{\mathfrak{A}}$, *jei* $a-b\in\mathfrak{A}$.

Sąryšis $a\equiv b \pmod{\mathfrak{A}}$ vadinamas *lyginiu* (arba kongruencija) *moduliu* $\mathfrak{A}$.

Lyginių mod $\mathfrak{A}$ savybės.

1. $(\forall a\in\check{Z})\ a\equiv a \pmod{\mathfrak{A}}$.

Ši savybė išplaukia iš teiginio $a-a=O\in\mathfrak{A}$.

2. *Jeigu* $a\equiv b \pmod{\mathfrak{A}}$, *tai ir* $b\equiv a \pmod{\mathfrak{A}}$.

Įrodymas. Jeigu $a-b\in\mathfrak{A}$, tai $O-(a-b)=b-a\in\mathfrak{A}$.

3. *Jeigu* $a\equiv b \pmod{\mathfrak{A}}$ *ir* $b\equiv c \pmod{\mathfrak{A}}$, *tai* $a\equiv c \pmod{\mathfrak{A}}$.

Įrodymas. Kadangi $a-b\in\mathfrak{A}$ ir $b-c\in\mathfrak{A}$, o $\mathfrak{A}$ yra požiedis, tai

$$(a-b)+(b-c)=a-c\in\mathfrak{A}.$$

Jeigu $a\equiv b \pmod{\mathfrak{A}}$ *ir* $c\equiv d \pmod{\mathfrak{U}}$, *tai*:
4. $a+c\equiv b+d \pmod{\mathfrak{A}}$ – *lyginius galima panariui sudėti,*
5. $a-c\equiv b-d \pmod{\mathfrak{A}}$ – *lyginius galima panariui atimti,*
6. $ac\equiv bd \pmod{\mathfrak{A}}$ – *lyginius galima panariui dauginti.*

Įrodymas. Jeigu $a-b\in\mathfrak{A}$ ir $c-d\in\mathfrak{A}$, o $\mathfrak{A}$ yra požiedis, tai:
$(a-b)+(c-d)=(a+c)-(b+d)\in\mathfrak{A}$,
$(a-b)-(c-d)=(a-c)-(b-d)\in\mathfrak{A}$,
$ac-bd=ac-ad+ad-bd=a(c-d)+a(a-b)\in\mathfrak{A}$.
Gautieji teiginiai rodo, kad 4–6 savybės teisingos.
Iš 5 savybės išplaukia šitokia išvada.

1 išvada. *Jeigu* $a+c\equiv b \pmod{\mathfrak{A}}$, *tai* $a\equiv b-c \pmod{\mathfrak{A}}$.
Ją gauname iš lyginio $a+c\equiv b \pmod{\mathfrak{A}}$ panariui atėmę lyginį $c\equiv c \pmod{\mathfrak{A}}$.

Iš 6 savybės išplaukia tokia išvada.

2 išvada. *Jeigu* $a\equiv b \pmod{\mathfrak{A}}$, *tai su kiekvienu natūriniu* $n\geqslant 2$ $a^n\equiv b^n \pmod{\mathfrak{A}}$ – *lyginio abi puses galima kelti natūriniu laipsniu.*

Įrodymas. Panariui sudauginę lyginius $a \equiv b \pmod{\mathfrak{A}}$ ir $a \equiv b \pmod{\mathfrak{A}}$, gauname $a^2 \equiv b^2 \pmod{\mathfrak{A}}$. Tarkime, kad $a^m \equiv b^m \pmod{\mathfrak{A}}$. Pastarąjį lyginį panariui padauginę iš lyginio $a \equiv b \pmod{\mathfrak{A}}$, gauname $a^{m+1} \equiv b^{m+1} \pmod{\mathfrak{A}}$. Dabar tereikia remtis matematinės indukcijos teorema.

7. *Jeigu* $f(x) = \sum_{k=0}^{n} a_k x^k$, $a_k \in \check{Z}$, $k = 0, 1, \ldots, n$ *ir* $c \equiv b \pmod{\mathfrak{A}}$, *tai* $f(c) \equiv f(b) \pmod{\mathfrak{A}}$.

Įrodymas. Jeigu $c \equiv b \pmod{\mathfrak{A}}$, tai $c^k \equiv b^k \pmod{\mathfrak{A}}$, $k = 0, 1, \ldots, n$. Kadangi $a_k \equiv a_k \pmod{\mathfrak{A}}$ ir $c^k \equiv b^k \pmod{\mathfrak{A}}$, tai

$$a_k c^k \equiv a_k b^k \pmod{\mathfrak{A}}, \quad k = 0, 1, \ldots, n.$$

Sudėję panariui, gauname

$$\sum_{k=0}^{n} a_k c^k \equiv \sum_{k=0}^{n} a_k b^k \pmod{\mathfrak{A}},$$

arba

$$f(c) \equiv f(b) \pmod{\mathfrak{A}}.$$

Įsitikinome, kad žiede sąryšio „*lygsta pagal idealą*“ savybės analogiškos sveikųjų skaičių žiedo sąryšio „*lygsta* (mod *m*)“ savybėms.

Pirmosios trys savybės reiškia, kad *sąryšis* „lygsta (mod $\mathfrak{A}$)“ yra *refleksyvus*, *simetrinis*, *tranzityvus*, taigi jis yra *ekvivalentumo* sąryšis. Pagal šį sąryšį žiedo bazinę aibę $\check{Z}$ galima suskirstyti į ekvivalentumo klases.

Žiedo $\check{Z}$ *ekvivalentumo klase* K_a *pagal idealą* $\mathfrak{A}$ *vadiname aibę elementų, kurie lygsta elementui a pagal idealą* $\mathfrak{A}$, t. y.

$$K_a = \{ b \mid b \equiv a \pmod{\mathfrak{A}} \}$$

Faktoraibėje $\check{Z}/\mathfrak{A}$ – žiedo $\check{Z}$ ekvivalentumo klasių pagal idealą $\mathfrak{A}$ aibėje apibrėžkime sudėtį ir daugybą šitaip:

$$K_a + K_b = K_{a+b}, \quad K_a \cdot K_b = K_{ab}.$$

101 teorema. *Struktūra* $(\check{Z}/\mathfrak{A}, +, \cdot)$ *yra žiedas. Jeigu* $\check{Z}$ *– žiedas su vienetu, tai ir* $(\check{Z}/\mathfrak{A}, +, \cdot)$ *yra žiedas su vienetu.*

Įrodymas. Tikrinsime, ar nagrinėjamoji struktūra turi žiedo apibrėžime nurodytas savybes.

Tarkime, kad a, b, c – bet kokie aibės $\check{Z}$ elementai. Pasinaudoję sudėties bei daugybos apibrėžimais ir tuo, kad $\check{Z}$ yra komutatyvusis žiedas, turime:

$$(K_a+K_b)+K_c=K_{a+b}+K_c=K_{(a+b)+c}=K_{a+(b+c)}=$$
$$=K_a+K_{b+c}=K_a+(K_b+K_c) \quad -\check{Z}.1.1;$$
$$K_a+K_O=K_{a+O}=K_{O+a}=K_O+K_a=K_a \quad -\check{Z}.1.2;$$
$$K_a+K_{-a}=K_{a+(-a)}=K_O; \quad -K_a=K_{-a} \quad -\check{Z}.1.3;$$
$$K_a+K_b=K_{a+b}=K_{b+a}=K_b+K_a \quad -\check{Z}.1.4;$$
$$(K_a\cdot K_b)\cdot K_c=K_{ab}\cdot K_c=K_{(ab)c}=K_{a(bc)}=K_a\cdot K_{bc}=K_a\cdot(K_b\cdot K_c) \quad -\check{Z}.2;$$
$$(K_a+K_b)\cdot K_c=K_{a+b}\cdot K_c=K_{(a+b)c}=$$
$$=K_{ac+bc}=K_{ac}+K_{bc}=K_a\cdot K_c+K_b\cdot K_c \quad -\check{Z}.3;$$
$$K_a\cdot K_b=K_{ab}=K_{ba}=K_b\cdot K_a \quad -\check{Z}.4.$$

Jeigu žiedas $\check{Z}$ turi vienetą e, tai $K_a\cdot K_e=K_{ae}=K_a$. Taigi K_e – vienetinė klasė.

Sukonstruotasis žiedas $\check{Z}/\mathfrak{A}$ *vadinamas žiedo* $\check{Z}$ *faktoržiedu pagal idealą* $\mathfrak{A}$.

Pavyzdžiai. 1. Jeigu $\check{Z}=Z$ – sveikųjų skaičių žiedas, o $\mathfrak{A}=(m)$, tai $Z/(m)=L_m$ – liekanų klasių moduliu m žiedas.

2. Jeigu $\mathfrak{A}=(0)$, tai $K_a=\{a\}$ ir $\check{Z}/(O)=\{\{a\} \mid a\in\check{Z}\}$. Šiuo atveju faktoržiedas nuo žiedo skiriasi tik tuo, kad vietoje elemento a rašoma aibė $\{a\}$.

3. Kai $\mathfrak{A}=\check{Z}$, yra tik viena klasė K_0, nes jei $a\in\check{Z}$, tai $O-a=-a\in\check{Z}$ ir $a\in K_0$. Šiuo atveju faktoržiedas yra trivialusis žiedas, kurio aibė turi tik vieną nulinį elementą.

Uždaviniai

14. Įrodykite šiuos teiginius:
1) Jeigu $\check{Z}$ yra žiedas su vienetu, tai $(a)=(-a)$;
2) Žiede su vienetu $(a)=(b)$ tada ir tik tada, kai a ir b – asocijuoti elementai;
3) Jeigu a yra žiedo vieneto daliklis, tai (a) – vienetinis idealas.

15. Jeigu K_a – ekvivalentumo klasė pagal idealą, tai $a\in K_a$.

16. Jeigu $b\in K_a$, $c\in K_a$, tai $K_b=K_c=K_a$.

17. Ekvivalentumo klasės K_a ir K_b lygios tada ir tik tada, kai $a\equiv b \pmod{\mathfrak{A}}$.

§54. Žiedų homomorfizmai

Vadovėlio pirmosios dalies 30 paragrafe buvo pateiktas žiedų homomorfizmo apibrėžimas ir aptartas homomorfizmo atskiras atvejis – izomorfizmas. Šiame paragrafe smulkiau nagrinėsime žiedų homomorfizmus.

Tarkime, kad $\check{Z}=(\check{Z},+,\cdot)$ ir $\check{Z}_1=(\check{Z}_1,+,\cdot)$ yra žiedai. Veiksmai, nors ir žymimi tais pačiais ženklais $+$ ir $\cdot$, gali būti skirtingi, nes ir pačios aibės $\check{Z}$ ir $\check{Z}_1$ gali skirtis viena nuo kitos. Pažymėkime O ir O_1 žiedų $\check{Z}$ ir $\check{Z}_1$ nulius, o e, e_1 – vienetus, jeigu jie yra tuose žieduose.

Funkcija f: $\check{Z}\to\check{Z}_1$, *turinti savybes*:

$$(\forall a,\ b\in\check{Z})\ f(a+b)=f(a)+(b),$$

$$f(ab)=f(a)\cdot f(b),$$

vadinama žiedo $\check{Z}$ *homomorfizmu žiede* $\check{Z}$, *kai* $f(\check{Z})\subset\check{Z}_1$ *ir* $f(\check{Z})\neq\check{Z}_1$, *arba žiedo* $\check{Z}$ *homomorfizmu į žiedą* $\check{Z}_1$, *kai* $f(\check{Z})=\check{Z}_1$.

Jeigu homomorfizmas yra bijekcija, tai jis vadinamas izomorfizmu (atitinkamai žiede arba į žiedą).

Kai egzistuoja bent vienas žiedo $\check{Z}$ *izomorfizmas į žiedą* $\check{Z}_1$, *tie žiedai vadinami izomorfiškais ir rašoma* $\check{Z}\cong\check{Z}_1$.

Pavyzdys. Funkcija f: $\mathbf{Z}\to\mathbf{L}_5$, apibrėžta formule $f(5t+r)=K_r$, $r=0, 1, 2, 3, 4$, K_r – liekanų klasė moduliu 5, yra sveikųjų skaičių žiedo homomorfizmas į žiedą $\mathbf{L}_5$.

102 teorema. *Sakykime,* f: $\check{Z}\to\check{Z}_1$ *yra homomorfizmas. Tada*: 1. $f(O)=O_1$; 2. $(\forall a\in\check{Z})\ f(-a)=-f(a)$; 3. *Jeigu žiedas* $\check{Z}$ *turi vienetą, tai ir žiedas* $\check{Z}_1$ *turi vienetą, ir* $f(e)=e_1$. 4. *Jeigu* a – *žiedo* $\check{Z}$ *su vienetu vieneto daliklis, tai* $f(a^{-1})=(f(a))^{-1}$.

Įrodymas. 1. Su bet kokiu $a\in\check{Z}$ $a+O=a$. Todėl $f(a)=f(a+O)=f(a)+f(O)$. Iš čia $f(O)=O_1$.

2. Kadangi $a+(-a)=O$ ir $f(a+(-a))=f(a)+f(-a)=O_1$, tai $f(-a)=-f(a)$.

3. Su bet kokiu $a\in\check{Z}$ $ae=a$. Todėl $f(a)=f(ae)=f(a)\cdot f(e)$. Iš čia $f(e)=e_1$.

4. Jeigu $a^{-1}\in\check{Z}$, tai $aa^{-1}=e$ ir $e_1=f(e)=f(a)\cdot f(a^{-1})$. Iš čia $f(a^{-1})=(f(a))^{-1}$.

103 teorema. *Žiedo* $\check{Z}$ *homomorfinis vaizdas žiede* $\check{Z}_1$ $f(\check{Z})$ *yra žiedo* $\check{Z}_1$ *požiedis.*

Įrodymas. Užtenka patikrinti 90 teoremos sąlygas. Imkime bet kokius a_1, $b_1\in f(\check{Z})$. Raskime tokius a, $b\in\check{Z}$, kad būtų

$$f(a)=a_1,\ f(b)=b_1.$$

Pasirėmę 102 teoremos 2 dalimi ir homomorfizmo apibrėžimu, gauname

$$a_1-b_1=a_1+(-b_1)=f(a)+\big(-f(b)\big)=f(a)+f(-b)=$$
$$=f\big(a+(-b)\big)=f(a-b)\in f(\check{Z}),$$
$$a_1b_1=f(a)f(b)=f(ab)\in f(\check{Z}).$$

Kai f: $\check{Z}\to\check{Z}_1$ *yra homomorfizmas, aibę* $H_a=\{b\mid f(b)=f(a),\ b\in\check{Z}\}$, *t. y. aibę tų elementų, kurių vaizdai sutampa su elemento* a *vaizdu, vadiname homomorfizmo* f *klase, generuota elemento* a.

Raskime homomorfizmo klasę, kurią generuoja žiedo $\check{Z}$ nulis – 0. Iš 102 teoremos 1 dalies išplaukia, kad

$$H_0 = \{b \mid f(b) = O_1,\ b \in \check{Z}\}.$$

Nulio generuota homomorfizmo f klasė H_0 vadinama homomorfizmo branduoliu ir žymima Ker f.

Taigi $\operatorname{Ker} f = \{b \mid f(b) = O_1,\ b \in \check{Z}\}$.
Branduolio vaidmuo išryškėja iš šios teoremos.

104 teorema. *Homomorfizmo f: $\check{Z} \to \check{Z}_1$ branduolys yra žiedo $\check{Z}$ idealas.*

Įrodymas. Pakanka patikrinti, ar aibėje $\operatorname{Ker} f \subset \check{Z}$ teisingos idealo apibrėžimo I. 1 ir I. 2 savybės.

Jeigu $a, b \in \operatorname{Ker} f$, tai $f(a) = O_1$ ir $f(b) = O_1$. Tada

$$f(a-b) = f\big(a+(-b)\big) = f(a) + f(-b) = f(a) - f(b) = O_1 - O_1 = O_1.$$

Taigi $a - b \in \operatorname{Ker} f$. Be to, su kiekvienu $z \in \check{Z}$

$$f(az) = f(a)f(z) = O_1 \cdot f(z) = O_1,$$

taigi $az \in \operatorname{Ker} f$. Teorema įrodyta.

105 teorema. $f(a) = f(b)$ *tada ir tik tada, kai*

$$a \equiv b \pmod{\operatorname{Ker} f}.$$

Įrodymas. Pakankamumas. Jeigu $a - b \in \operatorname{Ker} f$, tai $f(a-b) = O_1$. Bet $f(a-b) = f(a) - f(b)$, todėl $f(a) = f(b)$.

Būtinumas. Jeigu $f(a) = f(b)$, tai $f(a) - f(b) = f(a-b) = O_1$. Todėl $a - b \in \operatorname{Ker} f$. Tai reiškia, kad $a \equiv b \pmod{\operatorname{Ker} f}$.

Iš teoremos išplaukia, kad *homomorfizmo klasės sutampa su ekvivalentumo klasėmis pagal idealą* – Ker f.

106 teorema. *Jeigu f: $\check{Z} \to \check{Z}_1$ yra homomorfizmas, tai žiedo $\check{Z}$ faktoržiedas pagal* Ke *f izomorfiškas žiedo $\check{Z}$ homomorfiniam vaizdui $f(\check{Z})$:*

$$\check{Z}/\operatorname{Ker} f \cong f(\check{Z}).$$

Įrodymas. Apibrėžkime funkciją

$$\varphi\colon \check{Z}/\operatorname{Ker} f \to f(\check{Z})$$

lygybe $\varphi(H_a) = f(a)$. Pagal 105 teoremą ta funkcija yra bijekcija. Kadangi

$$\varphi(H_a + H_b) = \varphi(H_{a+b}) = f(a+b) = f(a) + f(b) = \varphi(H_a) + \varphi(H_b)$$

ir

$$\varphi(H_a \cdot H_b) = \varphi(H_{ab}) = f(ab) = f(a) \cdot f(b) = \varphi(H_a) \cdot \varphi(H_b),$$

tai bijekcija φ: $\check{Z}/\mathrm{Ker}\, f \leftrightarrow f(\check{Z})$ yra izomorfizmas.

Paėmę žiedo $\check{Z}$ idealą $\mathfrak{A}$ ir apibrėžę funkciją f: $\check{Z} \to \check{Z}/\mathfrak{A}$ lygybe $f(a) = K_a$, gausime žiedo $\check{Z}$ homomorfizmą į faktoržiedą $\check{Z}/\mathfrak{A}$. Tas homomorfizmas vadinamas *kanoniniu*.

Uždaviniai

18. Raskite sveikųjų skaičių žiedo $\mathbf{Z}$ homomorfizmą į liekanų klasių žiedą $\mathbf{L}_8$. Ar tas homomorfizmas kanoninis? Raskite jo branduolį ir ekvivalentumo klases pagal branduolį.

19. Liekanų klases moduliu 15 žymėkime K_r, o moduliu $5 - H_r$. Patikrinkite, ar funkcija $f(K_{5k+\rho}) = H_\rho$, $\rho = 0, 1, 2, 3, 4$, yra žiedo $\mathbf{L}_{15}$ homomorfizmas į žiedą $\mathbf{L}_5$. Raskite jo branduolį. Raskite ekvivalentumo klases pagal branduolį.

§55. Vyriausiųjų idealų žiedai

Integralumo sritis, kurios kiekvienas idealas yra vyriausias, vadinama vyriausiųjų idealų žiedu.

107 teorema. *Sveikųjų skaičių žiedas yra vyriausiųjų idealų žiedas.*

Įrodymas. $\{0\} = (0)$, todėl pakanka nagrinėti sveikųjų skaičių žiedo idealą $\mathfrak{A} \neq \{0\}$. Jame yra nelygių nuliui sveikųjų skaičių. Jeigu $k \in \mathfrak{A}$, tai ir $-k \in \mathfrak{A}$, todėl idealui priklauso ir natūrinių skaičių. Tegul d yra mažiausias natūrinis idealo $\mathfrak{A}$ skaičius. Paėmę bet kokį $a \in \mathfrak{A}$, turėsime $a = dq + r$, $0 \leqslant r < d$, ir $r = a - dq \in \mathfrak{A}$, todėl $r = 0$ ir $a = dq$. Taigi $\mathfrak{A} = \{dt \mid t \in Z\} = (d)$ – vyriausiasis idealas, kurį generuoja idealo $\mathfrak{A}$ mažiausias natūrinis skaičius.

108 teorema. *Kiekvienas vyriausiųjų idealų žiedas turi vienetinį elementą.*

Įrodymas. Jeigu $\check{Z}$ yra vyriausiųjų idealų žiedas, tai patį žiedą – vienetinį idealą generuoja kažkuris jo elementas a, t. y. $\check{Z} = (a)$, ir $a = ae$, $e \in \check{Z}$. Taigi

$$(\forall b \in \check{Z})(\exists q \in \check{Z})\ b = aq.$$

Tada $b = aq = aeq = (aq)e = be$, t. y. e – žiedo $\check{Z}$ vienetinis elementas.

109 teorema. *Vyriausiųjų idealų žiede* $\check{Z}$:
1. $b \mid a$ *tada ir tik tada, kai* $(a) \subset (b)$;
2. $(a) = (b)$ *tada ir tik tada, kai* a *ir* b *asocijuoti*;
3. $(a) = \check{Z}$ *tada ir tik tada, kai* a *– vieneto daliklis.*

Įrodymas. 1. Jeigu $b \mid a$, tai $a = bq$, $q \in \check{Z}$. Tada

$$(a) = \{at \mid t \in \check{Z}\} = \{bqt \mid t \in \check{Z}\} \subset \{bx \mid x \in \check{Z}\} = (b).$$

Jeigu $(a) \subset (b)$, tai $(\forall x \in \check{Z})(\exists u \in \check{Z})\ ax = bu$. Paėmę $x = e$, gauname $ae = a = bq$. Tai reiškia, kad $b \mid a$.

2 ir 3 teiginiai įrodomi analogiškai.

Remiantis šia teorema, dalumo sąryšį galima nagrinėti naudojantis idealais.

Vyriausiųjų idealų žiedo $\check{Z}$ *idealas* $\mathfrak{P} \neq \check{Z}$ *vadinamas pirminiu, jeigu iš sąlygos* $\mathfrak{P} \subset \mathfrak{A}$ *išplaukia* $\mathfrak{A} = \mathfrak{P}$ *arba* $\mathfrak{A} = \check{Z}$.

110 teorema. *Vyriausiųjų idealų žiede idealas* (p) *yra pirminis tada ir tik tada, kai* p *– pirminis elementas.*

Įrodymas. Būtinumas. Tarkime, kad $(p) \neq \check{Z}$ yra pirminis idealas, o $p = p_1 d$. Tada $(p) \subset (p_1)$ ir $(p) = (p_1)$ arba $(p_1) = \check{Z}$. Jeigu $(p_1) = (p)$, tai p ir p_1 – asocijuotieji elementai, ir todėl p_1 – netiesioginis p daliklis. Jeigu $(p_1) = \check{Z}$, tai p_1 yra vieneto daliklis. Taigi elementas p turi tik trivialiuosius daliklius. Vadinasi, jis yra pirminis.

Pakankamumas. Tarkime, kad p – pirminis elementas. Tada $(p) \neq \check{Z}$. Jeigu būtų $(p) \subset (d)$, tai p dalytųsi iš d ir d būtų arba vieneto daliklis, arba elementui p asocijuotas elementas. Kai d – vieneto daliklis, tada $(d) = \check{Z}$, kai d – elementui p asocijuotas elementas, tada $(d) = (p)$. Taigi (p) – pirminis idealas.

111 teorema. *Vyriausiųjų idealų žiedo faktoržiedas pagal pirminį idealą yra laukas.*

Įrodymas. Sakykime, $\check{Z}$ – vyriausiųjų idealų žiedas, $\mathfrak{P}$ – pirminis idealas, t. y. $\mathfrak{P} = (p)$, p – pirminis elementas. Įrodysime, kad yra tokia klasė $K_a \in \check{Z}/\mathfrak{P}$, kad $K_a K_u = K_e$, kai $K_a \in \check{Z}/\mathfrak{P}$ ir $K_a \neq \mathfrak{P}$.

Kadangi $\check{Z}$ – vyriausiųjų idealų žiedas ir $(a) \not\subset \mathfrak{P}$, tai pagal pirminio idealo apibrėžimą $(p) \subset (a, p) = \check{Z} = (e)$. Todėl yra tokie elementai u ir v, su kuriais $au + pv = e$. Bet tada $au - e = pv$, t. y. $au - e \in (p)$, arba $au \equiv e \pmod{\mathfrak{P}}$. Taigi $K_a K_u = K_e$ ir $K_u = K_a^{-1}$. Tai reiškia, kad faktoržiedo kiekvienas nenulinis elementas turi atvirkštinį. Taigi faktoržiedas yra laukas.

112 teorema. *Jeigu* p *yra vyriausiųjų idealų žiedo pirminis elementas ir* $p \mid ab$, *tai* $p \mid a$ *arba* $p \mid b$.

Įrodymas. Jeigu $p \nmid a$, tai samprotaudami taip pat kaip ir 111 teoremos įrodyme gausime lygybę

$$au + pv = e;$$

čia u, v – žiedo elementai.

Pastarąją lygybę padauginę iš b, gauname

$$abu + pbv = b.$$

Kadangi $p \mid ab$ ir $p \mid p$, tai $p \mid b$.

§56. Vyriausiųjų idealų žiedo elementų didžiausias bendrasis daliklis ir mažiausias bendrasis kartotinis

Vyriausiųjų idealų žiede galima nagrinėti sąvokas, kurios yra sveikųjų skaičių žiedo atitinkamų sąvokų bendriniai.

Prisiminę, kad sveikųjų skaičių $m_1, m_2, \ldots, m_n$ didžiausias bendrasis daliklis yra tų skaičių *bendrasis daliklis, kuris dalijasi iš kiekvieno tų skaičių bendrojo daliklio,* ir kad tų skaičių *mažiausias bendrasis* kartotinis yra toks jų *bendrasis kartotinis, iš kurio dalijasi kiekvienas tų skaičių bendrasis kartotinis,* nesunkiai suprasime toliau nagrinėjamas sąvokas.

Vyriausiųjų idealų žiedo elementų $a_1, a_2, \ldots, a_n$, tarp kurių bent vienas nelygus O, didžiausiu bendruoju dalikliu vadiname tokį jų bendrąjį daliklį, kuris dalijasi iš kiekvieno tų elementų bendrojo daliklio.

Kai $d \neq O$, tada $\varepsilon d \mid d$; čia ε — vieneto daliklis. Todėl pateiktasis apibrėžimas elementų $a_1, a_2, \ldots, a_n$ *didžiausią bendrąjį daliklį nustato vieneto daliklio tikslumu* — visą asocijuotųjų elementų klasę. Jį žymėsime $\mathrm{D}(a_1, a_2, \ldots, a_n)$.

113 teorema. *Jeigu $a_1, a_2, \ldots, a_n$ yra vyriausiųjų idealų žiedo elementai, tarp kurių bent vienas nelygus nuliui, tai tame pačiame žiede yra tokie elementai $u_1, u_2, \ldots, u_n$, kad*

$$\mathrm{D}(a_1, \ldots, a_n) \sim a_1 u_1 + \ldots + a_n u_n; \qquad (*)$$

čia ženklas $\sim$ reiškia „asocijuotieji elementai“.

Įrodymas. Nagrinėkime idealą $(a_1, a_2, \ldots, a_n)$, generuotą elementų $a_1, a_2, \ldots, a_n$. Kadangi žiedas yra vyriausiųjų idealų žiedas, tai jame yra toks elementas δ, kad

$$(a_1, \ldots, a_n) = (\delta).$$

Kadangi $\delta \in (a_1, a_2, \ldots, a_n)$, o kiekvienas idealo $(a_1, a_2, \ldots, a_n)$ elementas yra $\sum_{i=1}^{n} a_i x_i$ pavidalo, x_i — žiedo elementai, tai ir $\delta = \sum_{i=1}^{n} a_i u_i$, $u_1, u_2, \ldots, u_n$ — žiedo elementai. Iš pastarosios išraiškos išplaukia, kad δ dalijasi iš elementų $a_1, a_2, \ldots, a_n$ kiekvieno bendrojo daliklio d. Be to, kiekvienas $a_i \in (\delta)$, taigi dalijasi iš δ. Todėl ir δ yra elementų $a_1, a_2, \ldots, a_n$ bendrasis daliklis. Pagal apibrėžimą

$$\mathrm{D}(a_1, \ldots, a_n) \sim \delta = \sum_{i=1}^{n} a_i u_i.$$

Kadangi $\delta = a_1 u_1 + \ldots + a_n u_n \in Ž$, tai teisingas šitoks teiginys: *kiekvieni n ($n > 1$) vyriausiųjų idealų žiedo elementų $a_1, a_2, \ldots, a_n$, tarp kurių bent vienas nelygus nuliui, turi didžiausią bendrąjį daliklį.*

Atskiru atveju, kai $n=2$, paėmę a, $b\in\check{Z}$, $ab\neq O$, turėsime $D(a, b)\in\check{Z}$ ir rasime tokius u, $v\in\check{Z}$, su kuriais bus $D(a, b)\sim au+bv$.

Išraiška (*) *vadinama elementų* $a_1, \ldots, a_n$ *didžiausio bendrojo daliklio tiesine išraiška.*

Jeigu elementų a ir b didžiausias bendrasis daliklis yra vieneto daliklis, tai elementai a ir b vadinami tarpusavyje pirminiais.

114 teorema. *Vyriausiųjų idealų žiedo elementai a ir b tarpusavyje pirminiai tada ir tik tada, kai yra tokie to žiedo elementai u ir v, su kuriais teisinga lygybė*

$$au+bv=e.$$

Įrodymas. Jeigu a ir b — tarpusavyje pirminiai elementai, tai tokie u, $v\in\check{Z}$, su kuriais $au+bv=e$, egzistuoja pagal 113 teoremą.

Jeigu $au+bv=e$, tai kiekvienas a ir b bendrasis daliklis d yra vieneto e daliklis. Taigi a ir b — tarpusavyje pirminiai elementai.

1. Išvada. *Jeigu vyriausiųjų idealų žiede* $D(a, b)\sim\delta$, *tai* $a=\delta a_1$, $b=\delta b_1$, a_1 *ir* b_1 *— tarpusavyje pirminiai elementai.*

Įrodymas. Iš išraiškos $au+bv=\delta$ gauname $\delta a_1u+\delta b_1v=\delta$ ir $a_1u+b_1v=e$. Toliau pakanka remtis 114 teorema.

2. Išvada. *Jeigu vyriausiųjų idealų žiede* $c \mid ab$, b *ir* c *— tarpusavyje pirminiai elementai, tai* $c \mid a$.

Įrodymas. Lygybę $bu+cv=e$ padauginę iš a, gauname

$$(ab)u+c(av)=a.$$

Kadangi $c \mid ab$ *ir* $c \mid c$, tai ir $c \mid a$.

Vyriausiųjų idealų žiedo nenulinių elementų $a_1, a_2, \ldots, a_n$ *mažiausiu bendruoju kartotiniu* $M(a_1, \ldots, a_n)$ *vadiname jų bendrąjį kartotinį m, iš kurio dalijasi elementų* $a_1, a_2, \ldots, a_n$ *kiekvienas bendrasis kartotinis.*

Elementų $a_1, \ldots, a_n$ mažiausias bendrasis kartotinis, kaip ir didžiausias bendrasis daliklis, *apibrėžiamas vieneto daliklio tikslumu.*

115 teorema. *Vyriausiųjų idealų žiedo nenulinių elementų* $a_1, \ldots, a_n$ *bet kurio rinkinio mažiausias bendrasis kartotinis egzistuoja.*

Įrodymas. Idealų (a_i), $i=1, \ldots, n$, sankirta yra idealas (99 teorema), be to, vyriausiasis, nes žiedas yra vyriausiųjų idealų žiedas. Todėl yra toks žiedo elementas m, su kuriuo

$$(a_1) \cap \ldots \cap (a_n) = (m).$$

Kadangi $(m) \subset (a_i)$, tai $a_i \mid m$, $i=1, 2, \ldots, n$ (109 teorema). Todėl m yra elementų $a_1, \ldots, a_n$ bendrasis kartotinis. Jeigu m_1 yra koks nors elementų $a_1, \ldots, a_n$ bendrasis kartotinis, tai $m_1 = a_i t_i$, $i=1, \ldots, n$. Todėl $(m_1) \subset (a_i)$, $i=1, 2, \ldots, n$, taigi ir $(m_1) \subset (m) = (a_i) \cap \ldots \cap (a_n)$. Dabar telieka remtis 109 teorema ir apibrėžimu.

116 teorema. *Jeigu a, b, c — nenuliniai vyriausiųjų idealų žiedo elementai, tai* $\mathrm{M}(ac, bc) \sim c\mathrm{M}(a, b)$.

Įrodymas. Tarkime, kad $\mathrm{M}(a, b) \sim m$. Kadangi $m=ad$, $m=bh$, tai $mc=(ac)d$ ir $mc=(bc)h$. Vadinasi, mc yra elementų ac ir bc bendrasis kartotinis.

Imkime kokį nors elementų ac ir bc bendrąjį kartotinį m_1. Tada $m_1=act$, $m_1=bcs$, taigi ir

$$act = bcs.$$

Iš čia $at=bs$. Kadangi at dalijasi iš a ir iš b, tai at dalijasi ir iš $m \sim \mathrm{M}(a, b)$. Todėl $at=mu$ ir $m_1=act=atc=mcu$, taigi m_1 dalijasi iš mc. Todėl mc yra elementų ac ir bc mažiausias bendrasis kartotinis.

117 teorema. *Vyriausiųjų idealų žiedo tarpusavyje pirminių elementų a ir b mažiausias bendrasis kartotinis yra jų sandauga.*

Įrodymas. Aišku, kad ab yra elementų a ir b bendrasis kartotinis. Sakykime, m_1 — koks nors elementų a ir b bendrasis kartotinis. Tada $m_1=ac=bd$. Kadangi bd dalijasi iš a, o b ir a — tarpusavyje pirminiai elementai, tai pagal 114 teoremos antrąją išvadą d dalijasi iš a. Taigi $d=ah$. Tada

$$m_1 = bd = bah,$$

arba $ab \mid m_1$. Todėl $\mathrm{M}(a, b) \sim ab$.

118 teorema. *Vyriausiųjų idealų žiedo nenulinių elementų a ir b didžiausias bendrasis daliklis ir mažiausias bendrasis kartotinis susieti sąryšiu*

$$\mathrm{D}(a, b) \cdot \mathrm{M}(a, b) \sim ab.$$

Įrodymas. Tarkime, kad $\delta \sim \mathrm{D}(a, b)$ ir $m=\mathrm{M}(a, b)$. Tada $a=\delta a_1$, $b=\delta b_1$ ir a_1, b_1 — tarpusavyje pirminiai elementai pagal 114 teoremos pirmąją išvadą. Pagal 117 teoremą $\mathrm{M}(a_1, b_1) \sim a_1 b_1$, o pagal 116 teoremą $\mathrm{M}(a, b) = \mathrm{M}(\delta a_1, \delta b_1) \sim \delta a_1 b_1$. Iš čia

$$\delta m \sim b a_1 \delta b_1 = ab.$$

Įrodytosios didžiausio bendrojo daliklio ir mažiausio bendrojo kartotinio savybės yra sveikųjų skaičių didžiausio bendrojo daliklio ir mažiausio bendrojo kartotinio atitinkamų savybių analogai.

Uždaviniai

Vyriausiųjų idealų žiede įrodykite šitokius teiginius.

20. $D(ca_1, \ldots, ca_n) \sim cD(a_1, \ldots, a_n)$.

21. Jeigu $D(b, c) \sim e$, tai $D(ab, c) \sim D(a, c)$.

22. $D(a, b, c) \sim D(D(a, b), c)$.

23. $M(a, b, c) \sim M(M(a, b), c)$.

§57. Euklido žiedai

Vyriausiųjų idealų žieduose nėra algoritmo elementų didžiausiam bendrajam dalikliui (d. b. d.) ir mažiausiam bendrajam kartotiniui (m. b. k.) rasti. Kaip jau įsitikinome (§ 7 ir 8), sveikųjų skaičių žiede dalybos su liekana teorema ir iš jos išplaukiantis Euklido algoritmas leidžia rasti dviejų skaičių d. b. d. ir jo tiesinę išraišką, taip pat m. b. k. Analogiškus uždavinius, kaip matysime toliau, galime spręsti ir vadinamuosiuose Euklido žieduose — žieduose, kuriuose teisingas dalybos su liekana teoremos analogas.

$E = (E, +, \cdot)$ — *integralumo sritis. Jei egzistuoja funkcija*

$$g: E \setminus \{O\} \to \mathbf{N} \cup \{O\}$$

turinti savybes:

E.1. $g(ab) \geqslant g(a)$, *kai* $ab \neq O$,

E.2. *Kiekvienai elementų porai* $a, b \in E, b \neq O$, *egzistuoja tokie elementai* $q, r \in E$, *su kuriais teisinga lygybė*

$$a = bq + r$$

ir $r = O$ *arba* $g(r) < g(b)$, *tai integralumo sritis* E *vadinama Euklido žiedu.*

Pavyzdžiai. 1. Sveikųjų skaičių žiedas yra Euklido žiedas, nes E.1 ir E.2 savybes turi funkcija $g(k) = |k|$. E. 1 išplaukia iš lygybės $|km| = |k| \cdot |m|$, o E.2 — iš dalybos su liekana teoremos.

2. Gauso sveikųjų skaičių žiedas $\mathbf{Z}[i]$ yra Euklido žiedas.

Apibrėžkime $g(m+in) = m^2 + n^2$. Prisiminę, kad kompleksinių skaičių modulis turi savybę $|\alpha\beta| = |\alpha| \cdot |\beta|$, gauname $g((m+in)(k+il)) = g(m+in)\, g(k+il)$. Iš čia išplaukia E. 1 savybė. Kad įrodytume E. 2, imkime santykį

$$\frac{k+il}{m+in} = a + ib, \quad a, b \in Q.$$

Raskime tokius sveikuosius skaičius s, t, kad būtų $|a-s| \leqslant 1/2$ ir $|b-t| \leqslant 1/2$. Tada

$$\frac{k+il}{m+in} = s + it + (a-s) + i(b-t),$$

arba $k+il = (m+in)(s+it) + (m+in) \cdot ((a-s) + i(b-t))$. Aišku, kad $r = (m+in)((a-s) + i(b-t)) \in \mathbf{Z}[i]$. Be to, $g(r) = g(m+in)\, g((a-s) + i(b-t)) = g(m+in)((a-s)^2 + (b-t)^2) \leqslant g(m+in)((1/2)^2 + (1/2)^2) < g(m+in)$.

119 teorema. *Euklido žiedas yra vyriausiųjų idealų žiedas.*

Įrodymas. Kadangi $\{O\}=(0)$, tai užtenka įrodyti, kad kiekvienas nenulinis idealas yra vyriausiasis. Sakykime, $\mathfrak{A}\neq\{O\}$ ir $b\in\mathfrak{A}$ yra toks nenulinis elementas, su kuriuo $g(b)$ įgyja mažiausią reikšmę. Paėmę bet kokį $a\in\mathfrak{A}$, pagal E.2 gausime

$$a=bq+r \quad \text{ir} \quad r=O \quad \text{arba} \quad g(r)<g(b).$$

Kadangi $r=a-bq\in\mathfrak{A}$, tai tarę, kad $r\neq O$, gausime prieštaravimą b parinkimui. Todėl $r=O$. Bet tada

$$(\forall a\in\mathfrak{A})(\exists q\in E)\quad a=bq.$$

Iš čia išplaukia, kad

$$\mathfrak{A}=(b).$$

Išvados. 1. *Kiekvienas Euklido žiedas turi vienetinį elementą.*

2. *Euklido žiede teisingi visi teiginiai, kurie teisingi vyriausiųjų idealų žiede* (109–118 teoremos teisingos Euklido žiedams).

120 teorema. *Jeigu Euklido žiede $b\neq O$ yra netrivialus elemento a daliklis, tai $g(b)<g(a)$.*

Įrodymas. Kadangi b – netrivialus a daliklis, tai $a=bc$ ir $a\not\mid b$, t. y. $b=aq+r$, $g(r)<g(a)$. Tada $r=b-aq=b(e-cq)$ ir $g(r)=g(b(e-cq))\geqslant \geqslant g(b)$. Taigi $g(b)\leqslant g(r)<g(a)$.

Euklido algoritmas. *Euklido žiedo elementų a ir $b\neq 0$ Euklido algoritmu vadiname šitokį procesą, išplaukiantį iš* E.1 *ir* E.2 *savybių*:

0. $a=bq+r$, $g(r)<g(b)$;

1. $b=rq_1+r_1$, $g(r_1)<g(r)$;

2. $r=r_1q_2+r_2$, $g(r_2)<g(r_1)$;

. . . . . .

k – 1. $r_{k-3}=r_{k-2}q_{k-1}+r_{k-1}$, $g(r_{k-1})<g(r_{k-2})$;

k. $r_{k-2}=r_{k-1}q_k+r_k$, $r_k=O\vee g(r_k)=0$. (6.1)

Tai nuoseklus dalybos su liekana procesas. Kadangi $g(r)>g(r_1)>g(r_2)>$ $>\ldots$, tai tas procesas yra baigtinis. Po baigtinio žingsnių skaičiaus k gausime $g(r_k)=0$ arba $r_k=O$. Jeigu $r_k\neq O$, o $g(r_k)=0$, tai galėsime prirašyti dar vieną lygybę

$$r_{k-1}=r_kq_{k+1}.$$

Euklido žiede dviejų elementų a ir $b\neq 0$ didžiausią bendrąjį daliklį galima rasti naudojantis Euklido algoritmu.

121 teorema. *Euklido žiedo elementų a ir $b\neq 0$ didžiausias bendrasis daliklis yra asocijuotas tų elementų Euklido algoritmo paskutinei nelygiai nuliui liekanai.*

Įrodymas. Jeigu $c=dh+r$, tai pagal dalumo 7 ir 8 savybes elementų c ir d kiekvienas bendrasis daliklis yra ir elementų d ir r bendrasis daliklis, o elementų d ir r kiekvienas bendrasis daliklis yra ir elementų c ir d bendrasis daliklis. Iš to išplaukia, kad $\mathrm{D}(c, d)\sim\mathrm{D}(d, r)$.

Remdamiesi (6.1) Euklido algoritmu, gauname

$$\mathrm{D}(a, b)\sim\mathrm{D}(b, r)\sim\mathrm{D}(r, r_1)\sim\ldots\sim\mathrm{D}(r_{k-1}, r_k),$$

t. y. $\mathrm{D}(a, b)\sim\mathrm{D}(r_{k-1}, r_k)\sim\mathrm{D}(r_{k-2}, r_{k-1})$. Jeigu $r_k=0$, tai $r_{k-2}=r_{k-1}q_k$ ir $\mathrm{D}(r_{k-2}, r_{k-1})\sim r_{k-1}$. Jeigu $g(r_k)=0$, tai $r_{k-1}=r_kq_k$ ir $\mathrm{D}(r_{k-1}, r_k)\sim r_k$. r_{k-1} arba r_k yra paskutinė nelygi nuliui liekana. Taigi teorema įrodyta.

Pasinaudoję 121 teorema ir Euklido algoritmu, galime rasti ir tiesinę $\mathrm{D}(a, b)$ išraišką. Tarę, kad $r_k\neq O$, iš (6.1) k-osios lygybės išreiškiame r_k ir į gautąją lygybę įrašome išraišką, gautą iš $k-1$-osios lygybės. Pakartoję šią procedūrą, po k žingsnių gausime išraišką

$$\mathrm{D}(a, b)\sim r_k=au+bx.$$

Remiantis 120 teorema įrodomas pagrindinės aritmetikos teoremos analogas Euklido žieduose.

122 teorema. *Euklido žiede kiekvienas sudėtinis elementas turi pirminį daliklį.*

Įrodymas. Tarkime, kad a – sudėtinis elementas. Tada $a=a_1b_1$, a_1 ir b_1 – netrivialūs elemento a dalikliai. Pagal 120 teoremą $g(a_1)<g(a)$. Jeigu a_1 – pirminis elementas, tai teorema įrodyta. Jeigu a_1 – sudėtinis elementas, samprotavimą reikia kartoti. Taigi

$$a_1=a_2b_2 \quad \text{ir} \quad g(a_2)<g(a_1)<g(a).$$

Taip samprotaudami toliau, gausime

$$g(a_m)<\ldots<g(a_1)<g(a).$$

Kadangi $g(a_i)\in\mathbf{N}$, tai ta seka yra baigtinė. Todėl su tam tikru numeriu m a_m jau nėra sudėtinis elementas. Kadangi jis yra netrivialus a_{m-1} daliklis, tai a_m – pirminis elementas. Aišku, $a_m \mid a$.

Išvada. *Jeigu Euklido žiede* $\mathrm{D}(a, b)\sim e$, $\mathrm{D}(a, c)\sim e$, *tai ir* $\mathrm{D}(a, bc)\sim e$.

Įrodymas. Tarkime, kad $\mathrm{D}(a, bc)\sim d=pd_1$, p – pirminis elementas (toks yra pagal 121 teoremą, kai d nėra vieneto daliklis). Tada $p \mid a$ ir $p \mid bc$. Tarę, kad $p \mid b$, gautume $p \mid \mathrm{D}(a, b)$. To negali būti, nes $\mathrm{D}(a, b)\sim e$. Taigi $\mathrm{D}(p, b)\sim e$. Pagal 114 teoremos 2 išvadą $p \mid bc$, todėl $p \mid c$. Tada ir $p \mid \mathrm{D}(a, c)$. To negali būti, nes $\mathrm{D}(a, c)\sim e$. Prieštaravimo nebus tik tada, kai $\mathrm{D}(a, bc)\sim d$ bus vieneto daliklis.

123 teorema. *Jeigu p ir q yra pirminiai Euklido (vyriausiųjų idealų) žiedo elementai, tai teisingas tik vienas iš dviejų teiginių* – $\mathrm{D}(p, q)\sim e$ *arba* $q=\varepsilon p$, ε – *vieneto daliklis.*

Įrodymas. Galimi 2 atvejai: $p\nmid q$ ir $p \mid q$.

Jeigu $p\nmid q$, tai, remiantis pirminio elemento apibrėžimu, $\mathrm{D}(p, q)\sim e$.

Jeigu $p \mid q$, tai $q=pc$ ir $p=\varepsilon q$ arba $p=\varepsilon$, ε — vieneto daliklis. Bet $p=\varepsilon$ negali būti, nes p — pirminis elementas. Taigi lieka tik atvejis, kai $p=\varepsilon q$.

124 teorema. *Euklido žiede kiekvienas sudėtinis elementas išreiškiamas pirminių tame žiede elementų sandauga vieninteliu būdu (neatsižvelgiant į daugiklių tvarką ir vieneto daliklius).*

Pastaba. Posakis „vieninteliu būdu“ reiškia štai ką: *jeigu*

$$a=\prod_{j=1}^{k} p_j, \quad a=\prod_{j=1}^{s} q_j,$$

tai $k=s$ ir kiekvienam pirminiam elementui p_j yra asocijuotas pirminis elementas q_j kitoje sandaugoje.

Įrodymas. Tarkime, kad a — sudėtinis elementas. Pagal 122 teoremą jis turi pirminį daliklį p_1: $a=p_1a_1$. Jeigu a_1 yra pirminis, tai galime rašyti $a=p_1p_2$. Jeigu a_1 — sudėtinis, tai a_1 turi pirminį daliklį p_2: $a=p_1p_2a_2$.

Pakartoję samprotavimą $k-1$ kartą, gausime elementus $a=a_0$, a_1, ..., a_{k-1}, kurie pasižymi šitokia savybe: a_i yra netrivialus elemento a_{i-1} daliklis, $i=1, 2, \ldots, k-1$. Todėl pagal 120 teoremą

$$g(a_{k-1})<\ldots<g(a_1)<g(a).$$

Kadangi $g(a_i)\in\mathbf{N}$, tai ši seka yra baigtinė. Todėl galima rasti tokį $k\in\mathbf{N}$, kad būtų $a_{k-1}=p_k$, p_k — pirminis elementas.

Taigi $a=p_1p_2\ldots p_k$. Gavome sudėtinio elemento a išraišką pirminių elementų sandauga.

Išraiškos vienatį įrodysime matematinės indukcijos metodu.

1. Jeigu $a=p_1p_2$ ir $a=q_1q_2\ldots q_s$, tai $p_1p_2=q_1q_2\ldots q_s$. Kadangi $p_1 \mid q_1\ldots q_1$, tai pagal 122 teoremos išvadą ir 123 teoremą $p_1 \mid q_1$. Todėl $q_1=\varepsilon p_1$, ε — vieneto daliklis. Tada $p_2=\varepsilon q_2\ldots q_s$ ir $q_2=\varepsilon_1 p_2$. Iš to išplaukia $e=\varepsilon\varepsilon_1 q_3\ldots q_s$. Ta lygybė bus teisinga, kai dešinėje pusėje nebus pirminių daugiklių. Taigi $s=2$. Vadinasi, sudėtinio elemento a išraiška pirminių elementų sandauga yra vienintelė, kai a turi 2 pirminius daliklius.

2. Tarkime, kad minėtoji išraiška yra vienintelė, kai elementas a turi k pirminių daliklių. Iš lygybės

$$p_1p_2\ldots p_k=q_1q_2\ldots q_s$$

išplaukia, jog $k=s$ ir $q_i=\varepsilon_i p_i$, ε_i — vieneto dalikliai, $i=1, \ldots, k$.

3. Kai $p_1\ldots p_kp_{k+1}=q_1\ldots q_sq_{s+1}$, pagal 123 teoremą ir 122 teoremos išvadą $q_{s+1}=\varepsilon p_{k+1}$, ε — vieneto daliklis. Suprastinę abi lygybės puses iš p_{k+1}, gausime lygybę

$$p_1\ldots p_k=q_1\ldots q_s\varepsilon.$$

Dabar tereikia remtis prielaida.

124 teorema teisinga ir vyriausiųjų idealų žieduose. Tik jos įrodymas paremtas kitais principais ir faktais, apie kuriuos šioje knygoje nėra galimybės kalbėti. Įrodytoji 124 teorema nėra konstruktyvi, nes ji nenurodo būdo elemento išraiškai pirminių elementų sandauga rasti. O 121 teorema, taip pat Eu-

klido žiede teisinga 118 teorema yra konstruktyvios, nes pateikia būdą D (a, b) ir M (a, b) rasti. Trijų ir daugiau elementų d. b. d. ir m. b. k. galima rasti naudojantis rekurentinėmis formulėmis:

$$\mathrm{D}(a_1, \ldots, a_{n-1}, a_n) \sim \mathrm{D}\big(\mathrm{D}(a_1, \ldots, a_{n-1}), a_n\big),$$

$$\mathrm{M}(a_1, \ldots, a_{n-1}, a_n) \sim \mathrm{M}\big(\mathrm{M}(a_1, \ldots, a_{n-1}), a_n\big),$$

kurios su visais natūriniais $n \geqslant 3$ yra teisingos Euklido žiede.

Uždaviniai

24. Įrodykite, kad $\mathbf{Z}[\sqrt{2}]$ yra Euklido žiedas.

25. Raskite D (α, β) ir M (α, β) šių žiedo $\mathbf{Z}[i]$ elementų:
1) $\alpha = 5+7i$, $\beta = 1+2i$;
2) $\alpha = 4-5i$, $\beta = 2-i$;
3) $\alpha = -3+5i$, $\beta = 1-2i$.

26. Raskite D (α, β) ir M (α, β) šių žiedo $\mathbf{Z}[\sqrt{2}]$ elementų:
1) $\alpha = 5+2\sqrt{2}$, $\beta = 3+2\sqrt{2}$;
2) $\alpha = 7+3\sqrt{2}$, $\beta = 1+3\sqrt{2}$;
3) $\alpha = -8+5\sqrt{2}$, $\beta = 2+3\sqrt{2}$.

§58. Integralumo srities santykių laukas

Matematikoje sprendžiant įvairius uždavinius kartais pasitaiko tokia situacija, kai turimos aibės elementų neužtenka sprendiniams išreikšti. Iškyla aibės praplėtimo uždavinys.

Tarkime, kad $\check{\mathbf{Z}} = (\check{Z}, +, \cdot)$ yra integralumo sritis, kurios aibė $\check{Z}$ turi bent du skirtingus elementus, ir $a, b \in \check{Z}$. Nagrinėkime lygtį $bx = a$. Jeigu $b = O$, $a \neq O$, tai lygtis sprendinio neturi. Jeigu $a = O$, $b \neq O$, lygtis turi sprendinį $x = O$. Jeigu $a = O$ ir $b = O$, tai lygties sprendinys yra kiekvienas aibės $\check{Z}$ elementas. *Jeigu* $b \neq O$ ir $a \neq O$, *tai lygtis turi sprendinį, kai a dalijasi iš b*, t. y. kai aibėje $\check{Z}$ yra toks elementas q, kad $a = bq$. *Kai a nesidalija iš b, lygtis sprendinio neturi.*

Ar galima taip išplėsti aibę $\check{Z}$, kad naujojoje aibėje lygtis $bx = a$ turėtų sprendinį su kiekviena pora aibės $\check{Z}$ elementų $b \neq O$ ir a? Aišku, čia neužtenka praplėsti pačią aibę. Naujoje aibėje reikia taip apibrėžti sudėtį ir daugybą, kad poaibyje $\check{Z}$ tos operacijos liktų nepakitusios.

Šiame paragrafe, naudodamiesi aibių Dekarto daugyba ir aibės faktorizacija pagal ekvivalentumo sąryšį, sukonstruosime naują aibę. Toje aibėje tam tikru būdu apibrėžę sudėties ir daugybos operacijas, gausime lauką — integralumo srities viršlaukį. Viršlaukį konstruosime panašiai kaip racionaliųjų skaičių lauką.

Aibėje $\check{Z} \times (\check{Z} \setminus \{O\}) = \{(a, b) \mid a, b \in \check{Z}, b \neq O\}$ apibrėžiame sąryšį $\sim$ šitaip:

$$(a, b) \sim (c, d), \quad \text{kai} \quad ad = bc.$$

Kadangi $ab = ba$, tai $(a, b) \sim (a, b)$ — *sąryšis* $\sim$ *refleksyvus.*

Kai $ad = bc$, tai $cb = da$. Tai reiškia štai ką: jeigu $(a, b) \sim (c, d)$, tai ir $(c, d) \sim (a, b)$ — *sąryšis* $\sim$ *simetrinis.*

Jeigu $(a, b)\sim(c, d)$ ir $(c, d)\sim(g, h)$, tai

$$ad=bc \quad \text{ir} \quad ch=dg.$$

Padauginę šias lygybes atitinkamai iš h ir b, gausime

$$adh=bch \quad \text{ir} \quad chb=dgb.$$

Iš čia

$$adh=dgb, \quad \text{arba} \quad ah=gb.$$

Tai reiškia, kad $(a, b)\sim(g, h)$. Jeigu $(a, b)\sim(c, d)$ ir $(c, d)\sim(g, h)$, tai $(a, b)\sim$ $\sim(g, h)$. Taigi *sąryšis* $\sim$ *tranzityvus.*

Nustatėme, kad *sąryšis* $\sim$ yra *ekvivalentumo sąryšis aibėje* $\check{Z}\times(\check{Z}\setminus\{O\})$.

Pažymėkime $a/b=\{(c, d) \mid (c, d)\sim(a, b)\}$ ekvivalentumo klasę, kuriai priklauso (a, b), ir pavadinkime ją *elementų* a *ir* b *santykiu.*

Toks klasės žymėjimas nėra vienareikšmis, nes jei $(c, d)\sim(a, b)$, tai ir $(c, d)\sim(la, lb)$ su kiekvienu $l\neq O$ iš integralumo srities. Nevienareikšmiškumo išvengtume pareikalavę, kad elementai a ir b neturėtų bendrųjų daliklių. Bet tai tik komplikuotų reikalą.

Žymėjimo nevienareikšmiškumas netrukdys, nes vėliau apibrėžę klasių (santykių) veiksmus pamatysime, kad rezultatai nepriklauso nuo to, kaip žymėsime klasę.

Atkreipsime dėmesį, kad $a/b=ca/cb$ *su kiekvienu* $c\neq 0$. Iš tikrųjų $(a, b)\sim$ $\sim(ca, cb)$, nes $acb=bca$. Todėl ir klasės (santykiai) a/b ir ca/cd yra lygūs. Be to, $a/b=c/d$, kai $ad=bc$, nes tada $(a, b)\sim(c, d)$ ir jų apibrėžiamos ekvivalentumo klasės yra lygios.

Pažymėkime $\bar{Q}$ faktoraibę $\check{Z}\times(\check{Z}\setminus\{O\})/\sim$, t. y. integralumo srities $\check{Z}$ elementų santykių aibę. Šioje aibėje sudėtį ir daugybą apibrėžiame šitaip:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

Įsitikiname, kad suma ir sandauga nepriklauso nuo to, kaip pažymėtos klasės.

Tarkime, kad $\frac{a}{b}=\frac{a_1}{b_1}$ ir $\frac{c}{d}=\frac{c_1}{d_1}$, t. y. $ab_1=a_1b$ ir $cd_1=c_1d$. Tada

$$\frac{a_1}{b_1}+\frac{c_1}{d_1}=\frac{a_1d_1+c_1b_1}{b_1d_1}=\frac{a_1d_1bd+c_1b_1bd}{b_1d_1bd}=\frac{(a_1b)d_1d+(c_1d)b_1b}{b_1d_1bd}=$$

$$=\frac{ab_1d_1d+cd_1b_1d}{b_1d_1bd}=\frac{ad+cb}{bd}=\frac{a}{b}+\frac{c}{d}.$$

$$\frac{a_1}{b_1}\cdot\frac{c_1}{d_1}=\frac{a_1c_1}{b_1d_1}=\frac{a_1c_1bd}{b_1d_1bd}=\frac{(a_1b)(c_1d)}{b_1d_1bd}=\frac{ab_1cd_1}{b_1d_1bd}=\frac{ac}{bd}=\frac{a}{b}\cdot\frac{c}{d}.$$

125 teorema. *Kai integralumo srities* $\check{Z}$ *aibė* $\check{Z}$ *turi bent du skirtingus elementus, algebrinė struktūra* $(\bar{Q}, +, \cdot)$ *yra laukas.*

Įrodymas. Pakanka patikrinti lauko apibrėžime nurodytas sudėties ir daugybos savybes (žr. 1 d., § 31).

Akivaizdu, Card $\bar{Q}\geqslant$ Card $\check{Z}\geqslant 2$. Sudėties ir daugybos asociatyvumo ir komutatyvumo savybes, taip pat distributyvumo savybę paliekame įrodyti

skaitytojui. Čia įrodysime, kad egzistuoja nulinis, vienetinis, kiekvienam nenuliniam elementui atvirkštinis elementas.

Nulinį elementą rasime išsprendę lygtį

$$\frac{a}{b}+\frac{x}{y}=\frac{a}{b}.$$

Kadangi

$$\frac{a}{b}+\frac{x}{y}=\frac{ay+bx}{by}=\frac{a}{b},$$

tai $(ay+bx)b=aby$, $ab(y-y)+b^2x=O$. Iš čia išplaukia $x=O$, o y – bet koks nenulinis integralumo srities elementas. Taigi

$$O_{\overline{Q}}=\frac{O}{d},\quad d\neq O.$$

Vienetinį elementą rasime išsprendę lygtį

$$\frac{a}{b}\cdot\frac{x}{y}=\frac{a}{b},\quad a\neq 0,\quad b\neq 0,\quad y\neq O.$$

Gausime $\frac{ax}{by}=\frac{a}{b}$, $abx=aby$. Kadangi $ab\neq O$, tai $x=y$ – bet koks nelygus nuliui integralumo srities elementas. Taigi

$$e_{\overline{Q}}=\frac{d}{d},\quad d\neq O.$$

Jeigu $\frac{a}{b}\neq O_{\overline{Q}}$, tai $a\neq O$ ir $b\neq O$. Elementui a/b atvirkštinį elementą rasime išsprendę lygtį

$$\frac{a}{b}\cdot\frac{x}{y}=\frac{d}{d},\quad d\neq O.$$

Gauname $\frac{ax}{by}=\frac{d}{d}$, $adx=bdy$, $ax=by$. Vienas iš tos lygties sprendinių yra $x=b$, $y=a$. Taigi

$$\left(\frac{a}{b}\right)^{-1}=\frac{b}{a},\quad \text{kai}\quad a\neq O.$$

126 teorema. *Santykių* $\left\{\frac{ab}{b}\;\middle|\;a\in\check{Z},\ b\neq 0\right\}$ *aibė yra lauko* $(\overline{Q},\ +,\ \cdot)$ *požiedis, izomorfiškas integralumo sričiai* $\check{\mathbf{Z}}$.

Įrodymas. Apibrėžkime funkciją $f(ab/a)=a$. Ši funkcija yra aibės $\left\{\frac{ab}{b}\;\middle|\;a\in\check{Z},\ b\neq O\right\}$ bijekcija į aibę $\check{Z}$ ($ab/b=ad/d$, nes $abd=bad$). Kadangi

$$f\left(\frac{ab}{b}+\frac{cd}{d}\right)=f\left(\frac{abd+bcd}{bd}\right)=f\left(\frac{(a+c)bd}{bd}\right)=a+c=f\left(\frac{ab}{b}\right)+f\left(\frac{cd}{d}\right)$$

ir

$$f\left(\frac{ab}{b}\cdot\frac{cd}{d}\right)=f\left(\frac{acbd}{bd}\right)=ac=f\left(\frac{ab}{b}\right)\cdot f\left(\frac{cd}{d}\right),$$

tai bijekcija f yra izomorfizmas. Struktūra, izomorfiška integralumo sričiai, yra integralumo sritis (1 d., 23 teorema).

Aibės $\overline{Q}$ klases (santykius) ab/b pakeičiame elementais a ir gauname aibę

$$Q_{\check{Z}} = \overline{Q} \setminus \left\{ \frac{ab}{b} \mid a,\ b \in \check{Z},\ b \neq O \right\} \cup \check{Z}.$$

Sudėtį ir daugybą apibrėžiame šitaip:

$$a + \frac{c}{d} = \frac{ad+c}{d}, \quad a \cdot \frac{c}{d} = \frac{ac}{d}.$$

Akivaizdu, kad $\check{Z} \subset Q_{\check{Z}}$ ir *struktūra* $(Q_{\check{Z}}, +, \cdot)$ yra *laukas*. Jis vadinamas *integralumo srities* $\check{\mathbf{Z}}$ *santykių lauku*. Šio lauko elementai vadinami integralumo srities $\check{\mathbf{Z}}$ *elementų santykiais*. Keitinį $ab/b \leftrightarrow a$ laikysime sutapatinimu ir rašysime $ab/b = a$.

Kai integralumo sritis $\check{\mathbf{Z}}$ turi vienetą e, tada $ab/b = abe/be = ae/e = a/e = a$. Jeigu $a \neq O$ yra integralumo srities elementas, tai

$$a^{-1} = \left(\frac{a}{e}\right)^{-1} = \frac{e}{a} \in Q_{\check{Z}}.$$

Santykių lauko $Q_{\check{Z}}$ vienetas sutampa su integralumo srities vienetu, nes

$$\frac{d}{d} = \frac{de}{de} = \frac{e}{e} = \frac{ee}{e} = e,$$

o nulis sutampa su integralumo srities nuliu, nes

$$\frac{O}{d} = \frac{O \cdot d}{d} = O.$$

127 teorema. *Integralumo srities santykių laukas yra tos srities minimalusis viršlaukis.*

Įrodymas. Tarkime, kad $\check{\mathbf{Z}}$ yra integralumo sritis, $Q_{\check{Z}}$ – jos santykių laukas, o $\mathbf{L}$ – koks nors $\check{\mathbf{Z}}$ viršlaukis. Užtenka įrodyti, kad $Q_{\check{Z}} \subset \mathbf{L}$.

Kadangi $\check{Z} \subset L$, tai kiekviena pora $a, b \in \check{Z}$ priklauso ir viršlaukiui $\mathbf{L}$. Jeigu $b \neq O$, tai $b^{-1} \in L$ ir todėl

$$\frac{a}{b} = a \cdot b^{-1} \in L.$$

Taigi $Q_{\check{Z}} \subset L$.

128 teorema. *Izomorfiškų integralumo sričių* $\check{\mathbf{Z}}$ *ir* $\check{\mathbf{Z}}_1$ *santykių laukai* $\mathbf{Q}_{\check{Z}}$ *ir* $\mathbf{Q}_{\check{Z}_1}$ *yra izomorfiški.*

Įrodymas. Tarkime, kad bijekcija f: $\check{Z} \leftrightarrow \check{Z}_1$ yra integralumo srities $\check{\mathbf{Z}}$ izomorfizmas į sritį $\check{\mathbf{Z}}_1$. Apibrėžkime funkciją φ: $Q_{\check{Z}} \to Q_{\check{Z}_1}$ šitaip:

$$\varphi\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}.$$

Funkcija φ yra bijekcija, nes f yra bijekcija. Kadangi

$$\varphi\left(\frac{a}{b}+\frac{c}{d}\right)=\varphi\left(\frac{ad+bc}{bd}\right)=\frac{f(ad+bc)}{f(bd)}=\frac{f(ad)+f(bc)}{f(bd)}=$$

$$=\frac{f(a)f(d)+f(b)f(c)}{f(b)f(d)}=\frac{f(a)}{f(b)}+\frac{f(c)}{f(d)}=\varphi\left(\frac{a}{b}\right)+\varphi\left(\frac{c}{d}\right)$$

ir

$$\varphi\left(\frac{a}{b}\cdot\frac{c}{d}\right)=\varphi\left(\frac{ac}{bd}\right)=\frac{f(ac)}{f(bd)}=\frac{f(a)f(c)}{f(b)f(d)}=\frac{f(a)}{f(b)}\cdot\frac{f(c)}{f(d)}=\varphi\left(\frac{a}{b}\right)\varphi\left(\frac{c}{d}\right),$$

tai funkcija φ yra izomorfizmas. Taigi $Q_{\check{Z}}\cong Q_{\check{Z}_1}$.

Uždaviniai

27. $\mathbf{Z}$ – sveikųjų skaičių žiedas, $\mathbf{Z}_m=(m)$, $m\in\mathbf{N}$, – bet koks jo požiedis. Įrodykite, kad $Q_{\mathbf{Z}}=Q_{\mathbf{Z}_m}$.

28. Raskite santykių laukus šių žiedų:

1) $\mathbf{Z}[i]$; 2) $\mathbf{Z}[\sqrt{2}]$; 3) $\mathbf{Z}[\sqrt{3}]$.

Polinomų virš integralumo srities žiedai

§59. Vieno kintamojo polinomai virš integralumo srities

Algebros pagrindą ilgą laiką sudarė algebrinių lygčių

$$\sum_{j=0}^{n} a_j x^j = 0$$

sprendimo teorija. Dabartinėje algebroje ji tėra bendrosios struktūrų teorijos dalis. Viena iš svarbiausių problemų struktūrų teorijoje yra struktūrų praplėtimas. Jo esmė šitokia: turime aibę ir joje apibrėžtas vieną arba kelias operacijas ir norime sukonstruoti tos aibės plėtinį, kuriame galimos tokios operacijos, kurios turimoje aibėje sutaptų su jau apibrėžtomis, o naujoje aibėje turėtų tas pačias arba ir naujų savybių. 58 paragrafe sukonstravome integralumo srities viršlaukį — santykių lauką. Šiame skyriuje išmoksime integralumo sritį praplėsti į integralumo sritį naudodamiesi reiškiniais

$$a_0 + a_1 x + \ldots + a_n x^n,$$

kuriuose a_0, a_1, ..., a_n yra duotosios integralumo srities $\check{\mathbf{Z}}$ elementai, o x — tam tikras tos srities plėtinio elementas.

Visur šiame skyriuje laikysime, kad $\check{\mathbf{Z}}=(\check{Z}, +, \cdot)$ yra integralumo sritis su nelygiu nuliui vienetiniu elementu $e \neq O$, t. y. netrivialus neturintis nulio daliklių komutatyvusis žiedas su vienetu (e ir O — žiedo vienetinis ir nulinis elementai).

Tarkime, kad $x \in \check{Z}$ (x priklauso kokiam nors tos integralumo srities plėtiniui $\mathbf{Z}'$) ir yra toks elementas, su kuriuo apibrėžta daugyba $a \cdot x$ ir $ax^m = x^m a$, imant bet kokį sveikąjį neneigiamą skaičių m ir $a \in \check{Z}$ (be to, laikome $x^0 = e$).

Elementas $x \in \check{Z}$ vadinamas transcendentiniu $\check{\mathbf{Z}}$ atžvilgiu, jei iš lygybės

$$a_0 + a_1 x + \ldots + a_n x^n = O,$$

kurioje a_0, a_1, ..., a_n yra integralumo srities elementai, o n — bet koks neneigiamas sveikasis skaičius, išplaukia lygybės $a_0 = a_1 = \ldots = a_n = 0$.

Kai x transcendentinis integralumo srities $\check{\mathbf{Z}}$ atžvilgiu, reiškinys

$$f(x)=a_0+a_1x+\ldots+a_nx^n=\sum_{j=0}^{n}a_jx^j,$$

kuriame a_0, a_1, ..., a_n, $a_n\neq O$, n — neneigiamas sveikasis skaičius, yra tos integralumo srities elementai, vadinamas vieno kintamojo x n-ojo laipsnio polinomu virš $\check{\mathbf{Z}}$.

a_j, $a_j\in\check{Z}$ $(j=0, 1, \ldots, n)$, vadinami polinomo $f(x)$ koeficientais, o a_n vadinamas vyriausiuoju koeficientu. Skaičius n vadinamas polinomo $f(x)$ laipsniu ir žymimas $\deg(f)$.

Pavyzdžiai. 1. $f(x)=3-4x+5x^2-7x^5$ yra penktojo laipsnio polinomas virš sveikųjų skaičių žiedo **Z**.

2. $g(x)=x-2\sqrt{3}x^3+6\sqrt{5}x^4$ — ketvirtojo laipsnio polinomas virš realiųjų skaičių lauko **R**.

3. $h(x)=3-1/2i+(4-5i)x^3-8x^{19}$ (čia i — menamasis vienetas) — devynioliktojo laipsnio polinomas virš kompleksinių skaičių lauko **K**.

Aišku, kad polinomą $f(x)$ galime laikyti polinomu virš realiųjų skaičių lauko **R** arba polinomu virš kompleksinių skaičių lauko **K**, kai x yra transcendentinis atitinkamai **R** ir **K** atžvilgiu. Analogiškai polinomą $g(x)$ galime laikyti polinomu virš lauko **K**, kai x yra transcendentinis lauko **K** atžvilgiu.

Polinomo apibrėžime paėmę $n=0$ ir $a_0\neq O$, gausime reiškinį $f(x)=a_0$ — *nulinio laipsnio polinomą*. Taigi *integralumo srities kiekvienas nenulinis elementas yra vieno kintamojo nulinio laipsnio polinomas virš tos integralumo srities.* Integralumo srities nulinį elementą O vadinsime *nuliniu polinomu virš tos integralumo srities ir žymėsime $O(x)$*. Nuliniam polinomui nepriskiriame jokio laipsnio. *Nulinio polinomo visi koeficientai lygūs nuliui.*

Polinomo apibrėžime paėmę $a_0=O$, $a_1=e$ ir $n=1$, gauname polinomą $f(x)=x$. Vadinasi, *kiekvienas transcendentinis integralumo srities atžvilgiu elementas x yra pirmojo laipsnio polinomas virš tos srities.*

Vieno kintamojo x polinomų virš integralumo srities $\check{\mathbf{Z}}$ aibę žymėsime $\check{Z}[x]$.

Įsitikinome, kad $\check{Z}\subset\check{Z}[x]$ ir $x\in\check{Z}[x]$.

Uždaviniai

1. Nustatykite polinomų laipsnius n ir išrašykite jų koeficientus $a_0, a_1, \ldots, a_n$ eilės tvarka. Virš kokio skaičių žiedo arba lauko yra šie polinomai (i — menamasis vienetas):

a) $3x^3-8x^9+14x^5-28x^8+2-63x$;

b) $15-23x+31x^{11}-\frac{1}{2}x^8-\frac{5}{7}x^{10}$;

c) $3x+3x^5-17\sqrt{7}x^9+\frac{\sqrt{5}}{13}x^7-0{,}13$;

d) $0{,}(3)x^3-16\pi x^8+19{,}(1)x^{13}-3x^6-18x^5-7\pi+657{,}3x^2$;

e) $3i-(45-7i)x^9-\left(\frac{13}{2}+\frac{7}{5i}\right)x^6-8x^5+2ix^3-6x^8+2x^2$;

f) $(\pi+i)x-(2-\pi i)x^5+37x^{29}+3ix^{17}-(15-13i)x^{11}+(3-4i)-\frac{105}{79}x^{13}$?

Užrašykite tuos polinomus narių laipsnių didėjimo tvarka ir narių laipsnių mažėjimo tvarka.

2. Nustatykite, kurie iš šių polinomų yra lygūs:

$f(x)=3x^5-6x^4+3x^2-\pi x+3$,

$g(x)=-3x^2-\pi x+3+3x^2+3x^2-6x^4$,

$\varphi(x)=3-\pi x+3x^2+6x^4+3x^5$,

$h(x)=6x^4-\sqrt{2x}-7x^3-15+9x^2$,

$k(x)=9x^2-15-7x^3-\sqrt{2x}+6x^4$,

$\psi(x)=3x^5+6x^4+3x^2-\pi x+3$.

§60. Transcendentinio elemento egzistavimas. Polinomų aibės konstravimas

Kyla klausimas, ar egzistuoja aukštesnio negu nulinio laipsnio polinomai virš $\check{Z}$. Norėdami į jį atsakyti, turime išsiaiškinti, ar egzistuoja transcendentinis žiedo $\check{Z}$ atžvilgiu elementas.

Tuo tikslu nagrinėsime aibę sekų $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$, kuriose $a_j \in \check{Z}$ $(j=0, 1, \ldots, n)$ ir gali būti tik baigtinis skaičius $n \geqslant 0$ nelygių nuliui elementų. Lygiomis laikysime sekas su atitinkamai lygiais nariais.

Aibėje

$$\tilde{Z}=\{(a_0, a_1, \ldots, a_n, O, O, \ldots) \mid a_j \in \check{Z} \quad (j=0, 1, \ldots, n)\}$$

apibrėžiame išorinę daugybos operaciją $\tilde{Z} \times \tilde{Z} \to \tilde{Z}$ – sekos daugybą iš žiedo $\check{Z}$ elemento:

$$c(a_0, a_1, \ldots, a_n, O, O, \ldots)=(ca_0, ca_1, \ldots, ca_n, O, O, \ldots).$$

Be to, apibrėžiame dvi vidines binares sudėties ir daugybos operacijas:

$$(a_0, a_1, \ldots, a_n, O, O, \ldots)+(b_0, b_1, \ldots, b_m, O, O, \ldots)=$$

$$=(a_0+b_0, a_1+b_1, \ldots, a_N+b_N, O, O, \ldots), \quad N=\max\{n, m\},$$

$$(a_0, a_1, \ldots, a_n, O, O, \ldots)\cdot(b_0, b_1, \ldots, b_m, O, O, \ldots)=$$

$$=(c_0, c_1, \ldots, c_{n+m}, O, O, \ldots),$$

$$c_k=\sum_{i+j=k} a_i b_j \quad (k=0, 1, \ldots, n+m, \ a_i=O, \text{ kai } i>n, \ b_j=O, \text{ kai } j>m).$$

Apibrėžtųjų sudėties ir daugybos operacijų atžvilgiu aibė $\check{Z}$ *yra žiedas* (tai įrodyti paliekame skaitytojui).

Be to, aibė

$$Z_0=\{(a, O, O, \ldots, O, \ldots) \mid a \in \check{Z}\}$$

yra žiedo $\tilde{\mathbf{Z}}$ požiedis, nes

$$(a, O, O, \ldots)+(b, O, O, \ldots)=(a+b, O, O, \ldots),$$

$$(a, O, O, \ldots)\cdot(b, O, O, \ldots)=(ab, O, O, \ldots).$$

Bijekcija $a\leftrightarrow(a, O, O, \ldots)$ yra žiedų $\check{\mathbf{Z}}$ ir $\mathbf{Z}_0$ izomorfizmas. Todėl žiedo $\check{\mathbf{Z}}$ elementus $(a, O, O, \ldots)$ pakeitę juos atitinkančiais elementais a, apibrėžę sudėtį

$$a+(a_0, a_1, \ldots, a_n, O, O, \ldots)=(a+a_0, a_1, \ldots, a_n, O, O, \ldots)$$

ir daugybą

$$a\cdot(a_0, a_1, \ldots, a_n, O, O, \ldots)=(a_0, a_1, \ldots, a_{n-1}, aa_n, O, O, \ldots),$$

o sekų sudėtį ir daugybą apibrėžę tokiu pat būdu kaip ir žiede $\tilde{\mathbf{Z}}$, gauname žiedą $\mathbf{Z}'$. *Pastarasis izomorfiškas žiedui* $\tilde{\mathbf{Z}}$, *nes bijekcija*

$$\varphi(a)=(a, O, O, \ldots),$$

$$\varphi(a_0, a_1, \ldots, a_n, O, O, \ldots)=(a_0, a_1, \ldots, a_n, O, O, \ldots),$$

$$a_n\neq O,\ n\geqslant 1,$$

yra tų žiedų izomorfizmas.

Aišku, kad $\check{\mathbf{Z}}$ *yra žiedo* $\mathbf{Z}'$ *požiedis.*

Imkime žiedo $\mathbf{Z}'$ elementą $x=(O, e, O, O, \ldots)$. Kadangi $x^2=(O, O, e, O, O, \ldots)$, $x^3=(O, O, O, e, O, O, \ldots)$, $\ldots, x^j=(O, O, O, \ldots, O, e, O, O, \ldots)$ (vienetinis elementas e yra $j+1$-ojoje vietoje, $j\geqslant 1$), o $a_jx^j=(O, \ldots, O, a_j, O, O, \ldots)$ (a_j yra $j+1$-ojoje vietoje), tai kiekvieną seką $(a_0, a_1, \ldots, a_n, O, O, \ldots)$ $(n\geqslant 1)$ iš Z' galime užrašyti šitaip:

$$(a_0, a_1, \ldots, a_n, O, O, \ldots)=a_0+a_1x+\ldots+a_nx^n.$$

Kadangi $(a_0, a_1, \ldots, a_n, O, O, \ldots)=O$ žiede $\mathbf{Z}'$ tik tada, kai $a_0=a_1=\ldots=a_n=O$, tai $x=(O, e, O, O, \ldots)$ yra transcendentinis elementas integralumo srities $\check{\mathbf{Z}}$ atžvilgiu.

Taigi *kiekvienas žiedo* $\mathbf{Z}'$ *elementas yra polinomas virš* $\check{\mathbf{Z}}$.

Jeigu $x=(O, e, O, O, \ldots)$, tai su kiekvienu $n\geqslant 0$

$$\sum_{j=0}^{n} a_jx_j\ (a_j\in\check{Z},\quad j=0, 1, \ldots, n)$$

yra žiedo $\mathbf{Z}'$ elementas. Be to, $a\in\check{Z}$ taip pat yra žiedo $\mathbf{Z}'$ elementas. Todėl *aibė* Z' *— polinomų virš* $\check{\mathbf{Z}}$ *aibė*, t. y. $Z'=\check{Z}[x]$. *Ta polinomų aibė yra žiedas.*

Uždaviniai

3. Sakykime, x — transcendentinis elementas integralumo srities $\check{\mathbf{Z}}$ atžvilgiu. Įrodykite, kad su kiekvienu $n\in\mathbf{N}$ x^n yra transcendentinis elementas $\check{\mathbf{Z}}$ atžvilgiu.

4. Sukonstruokite polinomų aibę paėmę integralumo sritį — sveikųjų skaičių žiedą $\mathbf{Z}$.

§61. Algebrinė ir funkcinė polinomų lygybė

Kadangi polinomai virš integralumo srities $\check{Z}$ yra jos plėtinio – žiedo Z' elementai, o žiedo elementai yra lygūs tada, kai jų skirtumas lygus nuliui, tai ir du polinomai virš $\check{Z}$

$$f(x)=\sum_{j=0}^{n} a_j x^j,\ g(x)=\sum_{j=0}^{m} b_j x^j$$

yra lygūs, kai $f(x)-g(x)=O$ (čia O – žiedo Z', kartu ir $\check{Z}$ nulinis elementas). Lengvai įrodome šitokį teiginį.

Du polinomai virš $\check{Z}$ yra lygūs tada ir tik tada, kai lygūs jų atitinkami koeficientai.

Įrodymas. Sąlygos pakankamumas akivaizdus.

Būtinumas. Priminsime, kad žiede Z', kai $f(x)=g(x)$, gauname lygybę

$$f(x)-g(x)=\sum_{j=0}^{n} a_j x^j-\sum_{j=0}^{m} b_j x^j=\sum_{j=0}^{M} (a_j-b_j) x^j=0,$$

kurioje $M=\max\{n, m\}$ ir $a_j=O$, kai $j>n$, atitinkamai $b_j=O$, kai $j>m$. Kadangi $a_j-b_j\in\check{Z}$, o x – transcendentinis $\check{Z}$ atžvilgiu, tai

$$a_j-b_j=0,$$

t. y. $a_j=b_j$, $j=0, 1, \ldots, M$.

Kadangi $a_n\neq O$ ir $b_m\neq O$, tai iš tų lygybių gauname $n=m$. Taigi *lygių polinomų laipsniai yra lygūs.*

Polinomai $f(x)$ ir $g(x)$ lygūs, kai jų atitinkami koeficientai lygūs.

Konstruodami konkrečią polinomų aibę, neatsitiktinai ėmėme integralumo srities elementų seką. Juk iš polinomo apibrėžimo ir įrodytosios teoremos aišku, kad kiekvienas polinomas virš $\check{Z}$ apibrėžiamas jo koeficientais, nes kiekvieną polinomą abipus vienareikšmiškai atitinka jo koeficientų seka.

Jeigu

$$f(x)=\sum_{j=0}^{n} a_j x^j,\ g(x)=\sum_{j=0}^{m} b_j x^j,$$

t. y. $f(x)$ ir $g(x)$ yra n-ojo ir m-ojo laipsnio polinomai virš $\check{Z}$, tai polinomus $f(x)$ ir $g(x)$ galime užrašyti šitaip:

$$f(x)=\sum_{j=0}^{\infty} a_j x^j,\ g(x)=\sum_{j=0}^{\infty} b_j x^j; \tag{7.1}$$

čia $a_j = O$, kai $j > n$, ir $b_j = O$, kai $j > m$. Išrašę polinomų $f(x)$ ir $g(x)$ koeficientus kintamojo x laipsnių didėjimo tvarka, gausime sekas

$$(a_0, a_1, \ldots, a_n, O, O, \ldots), (b_0, b_1, \ldots, b_m, O, O, \ldots).$$

Tarp tokių sekų ir polinomų yra abipus vienareikšmė atitiktis, t. y.

$$f(x) \leftrightarrow (a_0, a_1, \ldots, a_n, O, O, \ldots).$$

$$g(x) \leftrightarrow (b_0, b_1, \ldots, b_m, O, O, \ldots).$$

Nustatėme, kad žiedo $\mathbf{Z}'$ elementų sekos irgi yra polinomai virš $\check{\mathbf{Z}}$. Susipažinę su polinomų lygybe, jų sudėtimi ir daugyba, nustatysime, kad anksčiau apibrėžta tokių sekų sudėtis ir daugyba užrašytąją bijekciją paverčia izomorfizmu.

Kai polinomų laipsniai žinomi arba kai nesvarbu, koks polinomo laipsnis, polinomus užrašysime (7.1) pavidalu. Toks užrašas patogus atliekant įvairias operacijas su polinomais ir nagrinėjant tų operacijų savybes.

Jeigu žiedas (arba laukas) $\bar{\mathbf{Z}}$ yra integralumo srities $\check{\mathbf{Z}}$ plėtinys, tai kiekvienas polinomas

$$f(x) = \sum_{j=0}^{n} a_j x^j$$

virš $\check{\mathbf{Z}}$ apibrėžia funkciją f: $\bar{Z} \to \bar{Z}$ šitaip:

$$(\forall z \in \bar{Z})\ f(z) = \sum_{j=0}^{n} a_j z^j.$$

Ta funkcija vadinama polinomine funkcija ir žymima $f(z)$.

Polinominės funkcijos reikšmę taške $z = l$ $(l \in \bar{Z})$

$$f(l) = \sum_{j=0}^{n} a_j l^j$$

(pagal tradiciją) vadinsime polinomo $f(x)$ reikšme taške l.

(Žinoma, tai jau yra tam tikra „kalbos laisvė“. Nėra prasmės kalbėti apie polinomo reikšmę, nes pagal apibrėžimą polinomas yra žiedo $\mathbf{Z}'$ konkretus elementas, kaip ir x – konkretus Z' elementas. Visur, kur kalbama apie polinomo reikšmę, reikia suprasti, kad turima omenyje polinominės funkcijos reikšmė.)

Aišku, kad polinominė funkcija

$$f\colon z \to \sum_{j=0}^{n} a_j z^j$$

apibrėžta ir aibėje $\check{Z}$, nes $\check{Z} \subset \overline{Z}$. Kadangi dvi funkcijos yra lygios, kai jų reikšmės sutampa kiekviename apibrėžimo srities taške, tai gali susidaryti įspūdis, kad lygiais polinomais galima laikyti tokius, kurių polinominės funkcijos lygios, t. y. tokius, kurių reikšmės sutampa kiekviename integralumo srities $\check{Z}$ taške. Tas įspūdis — klaidingas, nes tuo atveju, kai integralumo sritis $\check{Z}$ baigtinė, du skirtingi polinomai gali apibrėžti lygias polinomines funkcijas. Tai aiškiai matyti iš pavyzdžio.

Pavyzdys. Jeigu $f(x)=x^p-x$ ir $G(x)=K_0$ yra du polinomai virš liekanų pirminiu moduliu lauko $\mathbf{L}_p$ (integralumo srities $\mathbf{L}_p$), tai Ferma teoremos išvada (žr. III skyr., § 32) teigia, kad $f(K_r)=K_0$ su kiekviena klase $K_r \in L_p$. Taigi tie du nelygūs polinomai aibėje $\mathbf{L}_p$ apibrėžia lygias polinomines funkcijas.

Jeigu polinomai

$$f(x)=\sum_{j=0}^{n} a_j x^j, \quad g(x)=\sum_{j=0}^{m} b_j x^j$$

yra lygūs, tai jų apibrėžtos polinominės funkcijos taip pat lygios, nes su kiekvienu $l \in \overline{Z}$ teisinga lygybė

$$\sum_{j=0}^{n} a_j l^j = \sum_{j=0}^{n} b_j l^j$$

(iš polinomų lygybės išplaukia, kad $a_j=b_j$, $j=0, 1, \ldots, n$). Taigi lygių polinomų reikšmės sutampa kiekviename srities $\overline{Z}$ taške.

Polinomų lygybė paprastai vadinama algebrine polinomų lygybe. Jeigu polinominės funkcijos lygios, tai kalbama apie *funkcinę polinomų lygybę.*

Polinomų lygybę $f(x)=g(x)$ reikia skirti nuo analogiškai užrašytos lygties. Apie ką kalbama — lygybę ar lygtį, paaiškėja iš konteksto.

Uždaviniai

5. Apskaičiuokite polinomo $f(x)$ reikšmę taškuose l_j:

a) $f(x)=4x^3-6x^2+3x+1$, $l_1=0$, $l_2=-1$, $l_3=\sqrt{2}$;

b) $f(x)=3\sqrt{3}x^4+5x^3-2\sqrt{3}x^2-2\sqrt{3}$, $l_1=0$, $l_2=1$, $l_3=\sqrt{3}$;

c) $f(x)=(4+3i)x^3-(2-5i)x^2+(3-2i)x-7-5i$, $l_1=0$, $l_2=i$, $l_3=-i$, $l_4=1-i$.

6. Apskaičiuokite polinomo $f(x)=\sum_{j=0}^{n} a_j x^j \in \check{Z}[x]$ reikšmes taškuose $l_1=0$, $l_2=e$, $l_3=-e$.

Kad būtų trumpiau, susitarkime žymėti

$$r=K_r, \quad r=0, 1, \ldots, p-1,$$

liekanų klasę pirminiu moduliu p.

7. Tiesiogiai patikrinkite, ar polinomai $f(x)$ ir $g(x)$ virš lauko $\mathbf{L}_p$ apibrėžia lygias funkcijas lauke $\mathbf{L}_p$, kai:

1) $p=5$:

a) $f(x)=3x^2+2x+1$, $g(x)=2x^2+3x+1$;

b) $f(x)=4x^7+3x^6+2x^3+4x+2$, $g(x)=3x^3+2x^2+4x+2$;

c) $f(x)=3x^8+4x^5-2x+3$, $g(x)=3x^4+2x+3$;

2) $p=7$:

a) $f(x)=6x^4+4x^3+5x^2+2$, $g(x)=3x^5+2x^4+3x^3+3$;

b) $f(x)=x^7+6x^2+4x+1$, $g(x)=6x^2+5x+1$;

c) $f(x)=2x^9+4x^6+3x^3+2x^2+3$, $g(x)=4x^6+5x^3+2x^2+3$.

8. Įrodykite tvirtinimą: jeigu ne didesnio kaip n-ojo laipsnio polinomų f ir g virš skaičių lauko reikšmės sutampa bent $n+1$ taške, tai tie polinomai yra lygūs.

9. $(a_0, a_1, \ldots, a_n, 0, \ldots)$, $a_j \in \mathbf{R}$, $j=0, 1, \ldots, n$, $a_n \neq 0$, pavidalo sekų aibėje taip apibrėžkite binares sudėties ir daugybos operacijas, kad aibė sudarytų žiedą ir kad 61 paragrafe nustatytoji bijekcija virstų to žiedo izomorfizmu polinomų žiedui.

10. Raskite:

a) 2-ojo laipsnio polinomą, kai $f(0)=3$, $f(1)=2$, $f(-1)=-3$;

b) 2-ojo laipsnio polinomą, kai $f(1)=-18$, $f(-1)=-40$, $f(2)=-12$;

c) 3-ojo laipsnio polinomą, kai $f(1)=-5$, $f(-1)=-1$, $f(-3)=-5$, $f(3)=31$;

d) 4-ojo laipsnio polinomą, kai $f(0)=2$, $f(1)=4$, $f(-1)=8$, $f(2)=14$, $f(-2)=46$.

§62. Operacijos vieno kintamojo polinomų aibėje

Polinomų virš $\check{Z}$ aibę $\check{Z}[x]$ nagrinėsime joje įvedamų binarių operacijų savybių atžvilgiu. Susipažinsime su viena išorine binare operacija $\check{Z} \times \check{Z}[x] \to \check{Z}[x]$, vadinama *polinomų daugyba iš žiedo elementų*, ir su dviem vidinėmis binarėmis operacijomis — *polinomų sudėtimi ir daugyba*.

Polinomas

$$f(x)=\sum_{j=0}^{n} a_j x^j$$

dauginamas iš integralumo srities elemento c šitaip:

$$cf(x)=\sum_{j=0}^{n} (ca_j) x^j, \quad f(x)c=\sum_{j=0}^{n} (a_j c) x^j.$$

Pavyzdys. Jeigu $f(x)=3-6x+18x^5$, o $c=-5$, tai

$$cf(x)=-5f(x)=-15+30x-90x^5.$$

Akivaizdu, kad su kiekvienu integralumo srities elementu c ir su kiekvienu polinomu $f(x)$

$$cf(x)\in\check{Z}[x] \quad \text{ir} \quad f(x)\,c\in\check{Z}[x].$$

Skaitytojas, remdamasis apibrėžimu ir polinomų lygybe, gali lengvai įrodyti šitokias polinomo daugybos iš žiedo elementų savybes:

1. $(\forall f(x)\in\check{Z}[x])\ ef(x)=f(x)$;

2. $(\forall c\in\check{Z},\ f(x)\in\check{Z}[x])\ cf(x)=f(x)c$ – komutatyvumo;

3. $(\forall c,\ d\in\check{Z},\ f(x)\in\check{Z}[x])\ (cd)f(x)=c\,(df(x))$ – asociatyvumo.

Polinomų sudėtis.

Polinomų $f(x)=\sum_{j=0}^{n} a_j x^j$ *ir* $g(x)=\sum_{j=0}^{m} b_j x^j$ *suma vadiname polinomą*

$$f(x)+g(x)=\sum_{j=0}^{N}(a_j+b_j)\,x^j;$$

čia $N=\max\{n, m\}$, *kai* $m\neq n$. *Kai* $m=n$, N *yra didžiausias neneigiamas sveikasis skaičius, su kuriuo* $a_N+b_M\neq O$.

Pažymėsime, kad gali būti $N=0$ arba $f(x)+g(x)=O(x)$. Polinomų suma yra nulinis polinomas, kai su visais $j=0, 1, \ldots, n$ $a_j=-b_j$, nes tada $a_j+b_j=O$.

Trumpa polinomų sudėties taisyklė būtų šitokia.

Sudedant du polinomus, reikia sudėti jų atitinkamus koeficientus.

Iš šios taisyklės išplaukia, kad polinomų sudėtis yra vidinė binarė operacija aibėje $\check{Z}[x]$. Lengvai įsitikinsime, kad polinomų sudėtis turi (žiedo) grupės sudėties savybes.

Sakykime, kad $f(x)$, $g(x)$, $h(x)$ – bet kokie vieno kintamojo polinomai virš integralumo srities $\check{Z}$. Tada teisingi šie teiginiai:

Ž.1.1. $(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$ – *sudėtis asociatyvi*;

Ž.1.2. $f(x)+O(x)=f(x)$ – *sudėtis turi neutralųjį elementą* $O(x)$;

Ž.1.3. $(\exists\ -f(x)\in\check{Z}[x])\ f(x)+(-f(x))=O(x)$ – *kiekvienas polinomas turi simetrišką sudėties atžvilgiu polinomą – priešingąjį polinomą*;

Ž.1.4. $f(x)+g(x)=g(x)+f(x)$ – *sudėtis komutatyvi.*

Polinomų daugybos iš integralumo srities elemento ir polinomų sudėties operacijos susietos dar ir šitaip:

4. $(\forall c,\ d\in\check{Z},\ f(x)\in\check{Z}[x])\ (c+d)f(x)=cf(x)+df(x)$,

5. $(\forall c\in\check{Z},\ f(x),\ g(x)\in\check{Z}[x])\ c\,(f(x)+g(x))=cf(x)+cg(x)$.

Pastarąsias distributyvumo savybes paliekame įrodyti skatytojui.

Sugretinę savybes Ž.1.1 – Ž.1.4 bei 1 – 5 ir prisiminę vektorinės erdvės apibrėžimą tuo atveju, kai integralumo sritis yra laukas, **Ž=L**, gauname šitokį teiginį.

Vieno kintamojo polinomų virš lauko **L** *aibė su sudėtimi ir daugyba iš lauko elementų yra vektorinė erdvė virš lauko* **L**.

Kadangi polinomų lygybė konstatuojama įsitikinus, kad tų polinomų atitinkami koeficientai lygūs, tai išvardytos savybės išplaukia iš atitinkamų lygybių, kurios teisingos su bet kuriais integralumo srities elementais:

$$(a+b)+c=a+(b+c),\quad a+O=a,\quad a+(-a)=O,$$

$$\left(-f(x)=\sum_{j=0}^{n}(-a_j)x^j\right),\quad a+b=b+a.$$

Polinomų atimtis. Imkime

$$f(x)+h(x)=g(x),\quad \sum_j (a_j+c_j)x^j=\sum_j b_j x^j,$$

$a_j+c_j=b_j$; iš čia $c_j=b_j-a_j$. Taigi

$$h(x)=g(x)-f(x)=\sum_{j=0}^{N}(b_j-a_j)x^j;$$

čia $N=\max\{m, n\}$, kai $m\neq n$, ir didžiausias neneigiamas sveikasis skaičius, su kuriuo $b_N-a_N\neq O$, kai $m=n$.

Iš polinomo $g(x)$ *atimant polinomą* $f(x)$, *iš polinomo* $g(x)$ *koeficientų atimami polinomo* $f(x)$ *atitinkami koeficientai.*

Pavyzdžiai. Imkime du polinomus

$$f(x)=4-5x+6x^3+10x^5,\quad g(x)=3-6x+3x^3+4x^4-10x^5.$$

Jų suma $-f(x)+g(x)=7-11x+3x^2+6x^3+4x^4$, skirtumas $-g(x)-f(x)=-1-x+3x^3-6x^3+4x^4-20x^5$.

Praktiškai sudedant arba atimant polinomus, patartina surašyti juos vieną po kitu taip, kad atitinkami nariai būtų viename stulpelyje.

Polinomų daugyba.

Polinomų

$$f(x)=\sum_{j=0}^{n} a_j x^j \quad ir \quad g(x)=\sum_{t=0}^{m} b_t x^t$$

sandauga vadinamas polinomas

$$d(x)=f(x)\,g(x)=\sum_{k=0}^{n+m} d_k x^k,$$

kurio koeficientai

$$d_k=\sum_{j+t=k} a_j b_t, \quad k=0,\ 1,\ \ldots,\ n+m. \tag{7.2}$$

Iš apibrėžimo išplaukia, kad *polinomų daugyba yra vidinė binarė operacija aibėje* $\check{Z}[x]$.

Įsitikinsime, kad polinomų daugybai būdingos komutatyviojo žiedo daugybos savybės.

Sakykime, kad

$$f(x)=\sum_{j=0}^{n} a_j x^j,\ g(x)=\sum_{t=0}^{m} b_t x^t,\ h(x)=\sum_{u=0}^{s} h_u x^u$$

– bet kokie polinomai iš $\check{Z}[x]$. Tada teisingi šie teiginiai:

Ž.2. $\big(f(x),\ g(x)\big)h(x)=f(x)\big(g(x)h(x)\big)$ – *daugyba asociatyvi*;

Ž.3. $(f(x)+g(x))h(x)=f(x)h(x)+g(x)h(x)$ – *daugyba distributyvi sudėties atžvilgiu*;

Ž.4. $f(x)\,g(x)=g(x)\,f(x)$ – *daugyba komutatyvi.*

Įrodymas.

Ž.2. Polinomo $f(x)\,g(x)$ koeficientus žymėkime d_k, o $\big(f(x)\,g(x)\big)h(x)$ koeficientus – c_v. Pasinaudoję (7.2) formulėmis, gausime

$$d_k=\sum_{j+t=k} a_j b_t, \quad k=0,\ 1,\ \ldots,\ n+m,$$

ir

$$c_v=\sum_{k+u=v} d_k h_u=\sum_{k+u=v}\Big(\sum_{j+t=k} a_j b_t\Big) h_u=\sum_{j+t+u=v} a_j b_t h_u, \tag{7.3}$$

$$v=0,\ 1,\ \ldots,\ (n+m)+s.$$

Polinomo $g(x)\,\bar{h}(x)$ koeficientai tebūnie $\bar{d}_l$, o polinomo $f(x)\,(g(x)\times$ $\times h(x))$ koeficientai – $\bar{c}_v$. Analogiškai gauname

$$\bar{d}_l = \sum_{t+u=l} b_t h_u, \quad l=0,\ 1,\ \ldots,\ m+s,$$

ir

$$\bar{c}_v = \sum_{j+l=v} a_j \bar{d}_l = \sum_{j+l=v} a_j \sum_{t+u=l} b_t h_u = \sum_{j+t+u=v} a_j b_t h_u, \tag{7.4}$$

$$v=0,\ 1,\ \ldots,\ n+(m+s).$$

Iš (7.3) ir (7.4) išplaukia $c_v=\bar{c}_v$, $v=0, 1, \ldots, n+m+s$, todėl $\big(f(x)\,g(x)\big)\times$ $\times h(x)=f(x)\,\big(g(x)h(x)\big)$.

Ž.3. Pažymėkime polinomo $\big(f(x)+g(x)\big)h(x)$ koeficientus c_k, o $f(x)+$ $+g(x)$ koeficientus s_j. Pagal sudėties ir daugybos apibrėžimus

$$c_k = \sum_{j+u=k} s_j h_u = \sum_{j+u=k} (a_j+b_j) h_u = \sum_{j+u=k} a_j h_u + \sum_{j+u=k} b_j h_u, \tag{7.5}$$

$$k=0,\ 1,\ \ldots,\ N+s,\ N=\max\{n,\ m\}.$$

Polinomo $f(x)h(x)$ koeficientai tebūnie d_k, o polinomo $g(x)\,h(x)$ koeficientai – m_k. Tada polinomo $f(x)\,h(x)+g(x)\,h(x)$ koeficientai bus d_k+ $+m_k$. Pasinaudoję daugybos apibrėžimu, gausime

$$d_k+m_k = \sum_{j+u=k} a_j h_u + \sum_{j+u=k} b_j h_u, \tag{7.6}$$

$$k=0,\ 1,\ \ldots,\ N+s.$$

Iš (7.5) ir (7.6) išplaukia $c_k=d_k+m_k$, $k=0, 1, \ldots, N+s$, todėl $(f(x)+$ $+g(x))h(x)=f(x)h(x)+g(x)h(x)$.

Ž.4. Ši savybė išplaukia iš lygybių

$$\sum_{j+t=k} a_j b_t = \sum_{j+t=k} b_t a_j, \quad k=0,\ 1,\ \ldots,\ n+m.$$

Paėmę polinomą $I(x)=e$, pagal daugybos apibrėžimą gausime

$$f(x)\,I(x) = \sum_{j=0}^{n+0} a_j x^j = f(x),$$

nes polinomo $I(x)$ visi koeficientai lygūs nuliui, išskyrus laisvąjį narį, kuris lygus l. Taigi *polinomų daugyba turi neutraluįjį elementą.*

Iš polinomų daugybos apibrėžimo išplaukia, kad sandaugos $f(x)g(x)$ vyriausiasis koeficientas nelygus nuliui, t. y.

$$c_{n+m}=a_n b_m \neq O.$$

Taigi teisingi šie teiginiai.

1. *Nenulinių polinomų sandauga nelygi nuliui.*

2. *Polinomų sandaugos laipsnis lygus dauginamųjų laipsnių sumai*: $\deg(fg) = \deg(f) + \deg(g)$.

Apibendrindami visas įrodytąsias polinomų sudėties ir daugybos savybes, gauname šitokią teoremą.

129 teorema. *Vieno kintamojo polinomų virš integralumo srities* $\check{\mathbf{Z}}$ *polinomų aibė su sudėtimi ir daugyba – struktūra* $\check{\mathbf{Z}}[x] = (\check{Z}[x], +, \cdot)$ *yra integralumo sritis.*

Žiedas $\check{\mathbf{Z}}[x]$ *vadinamas vieno kintamojo polinomų virš* $\check{\mathbf{Z}}$ *žiedu.*

Remdamiesi polinomų veiksmų savybėmis, galime suformuluoti praktišką polinomų daugybos taisyklę.

Dauginant polinomą $f(x)$ *iš polinomo* $g(x)$, *polinomo* $f(x)$ *kiekvieną narį reikia padauginti iš polinomo* $g(x)$ *kiekvieno nario ir gautąsias sandaugas sudėti sutraukus panašiuosius narius.*

Šią taisyklę pagrįsime pastebėję, kad polinomo

$$f(x) = \sum_{j=0}^{n} a_j x^j$$

kiekvienas narys $a_j x^j$ yra polinomas. Taigi kiekvienas polinomas yra polinomų (narių) suma. Pasirėmę distributyvumo (Ž. 3) ir sudėties komutatyvumo savybėmis, įsitikiname, kad pateiktoji taisyklė yra teisinga.

Iš taisyklės išplaukia polinomų daugybos stulpeliu algoritmas, analogiškas daugiaženklių skaičių daugybos stulpeliu algoritmui.

Pavyzdys.

$$\begin{array}{r} f(x) = \quad 3 - 4x + 6x^3 \\ \underline{g(x) = -1 + 2x^2 - 5x^3} \\ -3 + 4x \quad - 6x^3 \\ \quad + 6x^2 - 8x^3 \quad + 12x^5 \\ \quad - 15x^3 + 20x^4 \quad - 30x^6 \\ \hline f(x)\,g(x) = -3 + 4x + 6x^2 - 29x^3 + 20x^4 + 12x^5 - 30x^6. \end{array}$$

Iš polinomų apibrėžimo išplaukia: *jeigu integralumo sritis* $\mathbf{Z}'$ *yra integralumo srities* $\check{\mathbf{Z}}$ *plėtinys ir* $x \in Z'$, *tai* $\check{Z} \subset \check{Z}[x] \subset Z'$.

Tolesnė teorema išryškina polinomų žiedo $\check{\mathbf{Z}}[x]$ vietą tarp visų integralumo srities $\check{\mathbf{Z}}$ plėtinių, turinčių transcendentinį $\check{\mathbf{Z}}$ atžvilgiu elementą x.

130 teorema. *Polinomų virš integralumo srities* $\check{\mathbf{Z}}$ *žiedas* $\check{\mathbf{Z}}[x]$ *yra minimalus ta prasme, kad nė vienas jo tiesioginis požiedis negali kartu būti žiedo* $\check{\mathbf{Z}}$ *plėtinys ir turėti elementą* x.

Įrodymas. Tarkime, kad $\mathbf{Z}_1$ yra žiedo $\check{\mathbf{Z}}[x]$ požiedis, kuriam priklauso elementas x ir kuris yra žiedo $\check{\mathbf{Z}}$ plėtinys. Tada $x^j \in Z_1$, $j \in \mathbf{N}$, o kiekvienas žiedo $\check{\mathbf{Z}}$ elementas a priklauso ir $\mathbf{Z}_1$. Tuomet su kiekvienu $n \geqslant 1$

$$\sum_{j=0}^{n} a_j x^j \in Z_1 \quad (a_j \in \check{Z},\ j=0,\ 1,\ \ldots,\ n).$$

Tai reiškia, kad $\check{Z}[x] \subset Z_1$. Taigi $\mathbf{Z}_1 = \check{\mathbf{Z}}[x]$.

Žiedas $\check{\mathbf{Z}}[x]$ gali turėti tokių požiedžių, kurie yra žiedo $\check{\mathbf{Z}}$ plėtiniai ir turi kurį nors kitą elementą $y \neq x$, transcendentinį žiedo $\check{\mathbf{Z}}$ atžvilgiu.

131 teorema. *Bet kurie du vieno kintamojo polinomų virš integralumo srities* $\check{\mathbf{Z}}$ *žiedai yra izomorfiški.*

Įrodymas. Jeigu x ir y – du skirtingi elementai, transcendentiniai integralumo srities $\check{\mathbf{Z}}$ atžvilgiu, tai bijekciją φ tarp polinomų žiedų $\check{\mathbf{Z}}[x]$ ir $\check{\mathbf{Z}}[y]$ nustatome šitaip: polinomui

$$\sum_{j=0}^{n} a_j x^j \in \check{\mathbf{Z}}[x]$$

priskiriame polinomą

$$\varphi\left(\sum_{j=0}^{n} a_j x^j\right) = \sum_{j=0}^{n} a_j y^j \in \check{\mathbf{Z}}[y],$$

t. y.

$$\varphi\big(f(x)\big) = f(y).$$

Iš polinomų sudėties ir daugybos savybių išplaukia, kad

$$\varphi\big(f(x)+g(x)\big) = f(y)+g(y),$$
$$\varphi\big(f(x)\,g(x)\big) = f(y)\,g(y).$$

Taigi ta bijekcija yra izomorfizmas.

Kadangi visi polinomų virš integralumo srities $\check{\mathbf{Z}}$ žiedai yra izomorfiški, tai galima nagrinėti bet kurį iš jų. Žymėjimuose $f(x)$ ir $\check{\mathbf{Z}}[x]$ simbolis x reikš bet kurį elementą iš plėtinio $\mathbf{Z}'$, transcendentinį $\check{\mathbf{Z}}$ atžvilgiu ir komutuojantį su kiekvienu integralumo srities $\check{\mathbf{Z}}$ elementu. Tai prasme x yra *kintamasis*, todėl polinomas $f(x)$ vadinamas *vieno kintamojo polinomu*, žiedas $\check{\mathbf{Z}}[x]$ – *vieno kintamojo polinomų žiedu.*

Uždaviniai

11. Apskaičiuokite polinomų f ir g sumą, skirtumą ir sandaugą:

a) $f(x)=3x-4$, $g(x)=5x^3+6x^2-2x+1$;

b) $f(x)=\sqrt{2}\,x^5-6x^2+3x+5$, $g(x)=13x-7+8x^3+3x^4-7x^5+10x^7$;

c) $f(x)=(2-i)\,x^3+6x^2-(1+i)\,x$, $g(x)=(\sqrt{2}-i)\,x^4+0{,}5x^2-(\sqrt{3}+2i)$;

d) $f(x)=(7+3i)x^5-6x^3+(5-7i)$, $g(x)=(13+i)-18x^2+(5-i)x^3+9x^4$.

12. Įrodykite šiuos teiginius:

a) $\check{\mathbf{Z}}[x] \supset \check{\mathbf{Z}}[x^2] \supset \check{\mathbf{Z}}[x^4] \supset \ldots \supset \check{\mathbf{Z}}[x^{2^k}]$; čia $k \in \mathbf{N}$ ir $\check{\mathbf{Z}}[x] \cong \check{\mathbf{Z}}[x^2] \cong \check{\mathbf{Z}}[x^4] \cong \ldots \cong \cong \check{\mathbf{Z}}[x^{2^k}]$, kai x – transcendentinis elementas integralumo srities $\check{\mathbf{Z}}$ atžvilgiu;

b) Su kiekvienu natūriniu m

$$\check{\mathbf{Z}}[x^{m^k}] \subset \check{\mathbf{Z}}[x^{(k-1)m}] \subset \ldots \subset \check{\mathbf{Z}}[x^{2m}] \subset \check{\mathbf{Z}}[x^m] \subset \check{\mathbf{Z}}[x],$$

ir visi tie žiedai yra izomorfiški. Čia $k \in \mathbf{N}$, x – transcendentinis elementas integralumo srities $\check{\mathbf{Z}}$ atžvilgiu;

c) Sakykime, $\mathbf{R}_n[x] = \left\{ \sum_{j=0}^{m} a_j x^j \mid a_j \in \mathbf{R},\ j = 0, 1, \ldots, m,\ m \leqslant n \right\}$. Įrodykite, kad $\mathbf{R}_n[x]$ yra $n+1$-matė vektorinė erdvė. Raskite kokią nors jos bazę.

§63. Kelių kintamųjų polinomų virš integralumo srities žiedai

Tarkime, kad $\mathbf{Z}'$ yra bet kuris integralumo srities $\check{\mathbf{Z}}$ plėtinys – integralumo sritis arba laukas. Imkime $x_1 \in \mathbf{Z}'$, transcendentinį $\check{\mathbf{Z}}$ atžvilgiu, ir sudarykime vieno kintamojo polinomų virš $\check{\mathbf{Z}}$ žiedą $\check{\mathbf{Z}}[x_1]$ – integralumo sritį. Tas žiedas taip pat turi plėtinį, kuriam priklauso elementas x_2, transcendentinis $\check{\mathbf{Z}}[x_1]$ atžvilgiu. Tokį plėtinį žymėsime taip pat $\mathbf{Z}'$. Jį galime sukonstruoti 60 paragrafe išdėstytu būdu.

Remdamiesi 59–62 paragrafuose gautais rezultatais, galime sudaryti žiedą $\check{\mathbf{Z}}[x_1][x_2]$, kurį žymėsime $\check{\mathbf{Z}}[x_1, x_2]$. Iš 130 ir 131 teoremų išplaukia, kad tas žiedas nustatomas vienareikšmiškai izomorfizmo tikslumu ir yra žiedo $\check{\mathbf{Z}}[x_1]$ minimalusis plėtinys, turintis elementą x_2, transcendentinį $\check{\mathbf{Z}}[x_1]$ atžvilgiu. *Žiedas* $\check{\mathbf{Z}}[x_1, x_2]$ *vadinamas dviejų kintamųjų* x_1 *ir* x_2 *polinomų virš* $\check{\mathbf{Z}}$ *žiedu.* Jo elementai (žr. polinomo apibrėžimą) yra šitokio pavidalo:

$$f(x_1, x_2) = \sum_{j=0}^{m} f_j(x_1) x_2^j,\ f_j(x_1) \in \check{\mathbf{Z}}[x_1] \quad (j = 0, 1, \ldots, m;\ m \geqslant 0).$$

Analogiškai samprotaudami, po n ($n \geqslant 1$) žingsnių gausime integralumo sritį

$$\check{\mathbf{Z}}[x_1, \ldots, x_{n-1}][x_n] = \check{\mathbf{Z}}[x_1, \ldots, x_n],$$

vadinamą n *kintamųjų* $x_1, x_2, \ldots, x_n$ *polinomų virš integralumo srities* $\check{\mathbf{Z}}$ *žiedu.* Tas žiedas yra žiedo $\check{\mathbf{Z}}[x_1, \ldots, x_{n-1}]$ minimalusis plėtinys, turintis transcendentinį žiedo $\check{\mathbf{Z}}[x_1, \ldots, x_{n-1}]$ atžvilgiu elementą x_n. *Kiekvienas žiedo* $\check{\mathbf{Z}}[x_1, \ldots, x_n]$ *elementas vadinamas* n *kintamųjų polinomu* ir yra šio pavidalo:

$$f(x_1, \ldots, x_n) = \sum_{j=0}^{m} f_j(x_1, \ldots, x_{n-1}) x_n^j; \tag{7.7}$$

čia $f \in \check{\mathbf{Z}}[x_1, \ldots, x_{n-1}]$ $(j = 0, 1, \ldots, m;\ m \geqslant 0)$.

Pavyzdys. Kai $\check{\mathbf{Z}}=\mathbf{Z}$, reiškinys

$$f(x, y)=(x^3+2)+(4x^2-5x)y+(16x^{23}-43x^{15}+18x)y^2$$

yra dviejų kintamųjų polinomas (su sveikaisiais koeficientais) iš $\mathbf{Z}[x, y]$.
Reiškinys

$$g(x, y, z)=(x+1)y-6y^3z+8xyz^3$$

yra trijų kintamųjų polinomas (su sveikaisiais koeficientais) iš $\mathbf{Z}[x, y, z]$.

Kadangi n kintamųjų polinomai virš $\check{\mathbf{Z}}$ yra vieno kintamojo polinomai virš $\check{\mathbf{Z}}[x_1, \ldots, x_{n-1}]$, tai *polinomų lygybė ir operacijos su jais apibrėžiamos visai taip pat kaip ir vieno kintamojo polinomams* (tik nereikia užmiršti, kad koeficientai yra polinomai).

Kad būtų patogiau, n kintamųjų polinomą iš $\check{\mathbf{Z}}[x_1, \ldots, x_n]$ žymėkime šitaip:

$$f=f(x_1, \ldots, x_n)=\sum_{j=0}^{m} f_j(x_1, \ldots, x_{n-1})x_n^j=\sum_{j=0}^{m} f_j x_n^j=\sum_j f_j x_n^j;$$

čia $f\in\check{Z}[x_1, \ldots, x_{n-1}]$ $(j=0, 1, \ldots, m)$, $f_j=0$, kai $j>m$.

Tada

$$\left(\sum_j f_j x_n^j=\sum_j g_j x_n^j\right)\Leftrightarrow(f_j=g_j,\quad j=0, 1, \ldots),$$

$$\sum_j f_j x_n^j+\sum_j g_j x_n^j=\sum_j (f_j+g_j)x_n^j,$$

$$\left(\sum_j f_j x_n^j\right)\left(\sum_j g_l g_n^l\right)=\sum_k\left(\sum_{j+l=k} f_j g_l\right)x_n^k.$$

132 teorema. *Kiekvieni du n kintamųjų polinomų virš integralumo srities žiedai yra izomorfiški.*

Įrodymas. Nagrinėkime du n kintamųjų virš $\check{\mathbf{Z}}$ žiedus

$$\mathbf{Z}_1=\check{\mathbf{Z}}[x_1, \ldots, x_n] \quad \text{ir} \quad \mathbf{Z}_2=\check{\mathbf{Z}}[y_1, \ldots, y_n].$$

Apibrėžkime funkciją

$$\varphi\colon \mathbf{Z}_1\to\mathbf{Z}_2$$

šitaip:

$$\varphi\left(f(x_1, \ldots, x_n)\right)=f(y_1, \ldots, y_n).$$

Ta funkcija yra bijekcija. Kadangi abiejuose polinomų žieduose sudėtis ir daugyba apibrėžtos vienodai, tai

$$\varphi\left(f(x_1, \ldots, x_n)+g(x_1, \ldots, x_n)\right)=f(y_1, \ldots, y_n)+g(y_1, \ldots, y_n)=$$
$$=\varphi\left(f(x_1, \ldots, x_n)\right)+\varphi\left(g(x_1, \ldots, x_n)\right),$$
$$\varphi\left(f(x_1, \ldots, x_n)\cdot g(x_1, \ldots, x_n)\right)=f(y_1, \ldots y_n)\cdot g(y_1, \ldots, y_n)=$$
$$=\varphi\left(f(x_1, \ldots, x_n)\right)\cdot\varphi\left(g(x_1, \ldots, x_n)\right).$$

Taigi φ: $Z_1\leftrightarrow Z_2$ yra izomorfizmas.

§64. Kelių kintamųjų polinomų normalusis pavidalas

Operuoti (7.7) pavidalo reiškiniais ne visada patogu, todėl stengsimės gauti kitą kelių kintamųjų polinomo virš $\check{Z}$ išraišką.

133 teorema. *Kiekvieną n kintamųjų ($n \geqslant 1$) polinomą f virš $\check{Z}$ galima išreikšti šitaip:*

$$f(x_1, \ldots, x_n) = \sum_{j_1 \ldots j_n} a_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n}; \qquad (7.8)$$

čia $a_{j_1 \ldots j_n}$ yra integralumo srities $\check{Z}$ elementai, iš kurių nelygių nuliui yra tik baigtinis skaičius; sumuojama pagal tuos neneigiamus indeksus $j_1, \ldots, j_n$, su kuriais $a_{j_1 \ldots j_n} \neq 0$. (7.8) pavidalo išraiška yra vienintelė.

Įrodymas. Teoremos pirmąją dalį įrodysime matematinės indukcijos metodu.

Kai $n=1$, (7.8) išraiška teisinga pagal vieno kintamojo polinomo apibrėžimą.

Tarkime, kad ta išraiška teisinga, kai $n=r$ ($r \geqslant 1$). Kai $n=r+1$,

$$f(x_1, \ldots, x_{r+1}) = \sum_{j=0}^{m} f_j(x_1, \ldots, x_r) x_{r+1}^j.$$

Pagal prielaidą

$$f_j(x_1, \ldots, x_r) = \sum_{j_1 \ldots j_r} a^{(j)}_{j_1 \ldots j_r} x_1^{j_1} \ldots x_r^{j_r} \quad (j=0, 1, \ldots, m).$$

Iš tų išraiškų išplaukia

$$f(x_1, \ldots, x_{r+1}) = \sum_{j=0}^{m} \sum_{j_1 \ldots j_r} a^{(j)}_{j_1 \ldots j_r} x_1^{j_1} \ldots x_r^{j_r} x_{r+1}^j.$$

Laikydami $a^{(j)}_{j_1 \ldots j_r} = O$, kai $j > m$, ir žymėdami $j = j_{r+1}$, $a^{(j)}_{j_1 \ldots j_r} = a_{j_1 \ldots j_{r+1}}$, galime užrašyti:

$$f(x_1, \ldots, x_{r+1}) = \sum_{j_1 \ldots j_{r+1}} a_{j_1 \ldots j_{r+1}} x_1^{j_1} \ldots x_r^{j_r} x_{r+1}^{j_{r+1}}.$$

Taigi tarus, kad (7.8) išraiška yra teisinga, kai $n=r$, išeina, jog ji teisinga ir kai $n=r+1$. Todėl ta išraiška teisinga su kiekvienu $n \geqslant 1$.

Įrodysime (7.8) išraiškos vienatį.

n kintamųjų polinomų aibė $\check{Z}[x_1, \ldots, x_n]$ su sudėtimi ir daugyba yra integralumo sritis. Dėmenys $a_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n}$ (7.8) išraiškoje yra to žiedo elementai. Pasinaudoję komutatyviojo žiedo binarių operacijų savybėmis, gaunamе šitokias (7.8) pavidalo reiškinių (polinomų) sudėties ir atimties taisykles:

Jeigu

$$f(x_1, \ldots, x_n) = \sum_{j_1 \ldots j_n} a_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n},$$

$$g(x_1, \ldots, x_n) = \sum_{j_1 \ldots j_n} b_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n},$$

tai

$$f(x_1, \ldots, x_n) \pm g(x_1, \ldots, x_n) = \sum_{j_1 \ldots j_n} (a_{j_1 \ldots j_n} \pm b_{j_1 \ldots j_n}) x_1^{j_1} \ldots x_n^{j_n}. \quad (7.9)$$

Tarkime, kad polinomas $f(x_1, \ldots, x_n)$ išreiškiamas dar ir šitaip:

$$f(x_1, \ldots, x_n) = \sum_{j_1 \ldots j_n} \tilde{a}_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n}.$$

Pastarąją išraišką atimame iš (7.8) ir, remdamiesi (7.9) lygybe, gauname

$$\sum_{j_1 \ldots j_n} (a_{j_1 \ldots j_n} - \tilde{a}_{j_1 \ldots j_n}) x_1^{j_1} \ldots x_n^{j_n} = 0. \quad (7.10)$$

Kadangi x_n yra transcendentinis elementas $\check{\mathbf{Z}}[x_1, \ldots, x_{n-1}]$ atžvilgiu, tai pastaroji lygybė teisinga tik tada, kai

$$\sum_{j_1 \ldots j_{n-1}} (a_{j_1 \ldots j_n} - \tilde{a}_{j_1 \ldots j_n}) x_1^{j_1} \ldots x_{n-1}^{j_{n-1}} = 0$$

su visais j_n.

Kadangi x_{n-1} yra transcendentinis elementas $\check{\mathbf{Z}}[x_1, \ldots, x_{n-2}]$ atžvilgiu, tai (7.10) lygybė teisinga tik tada, kai

$$\sum_{j_1 \ldots j_{n-2}} (a_{j_1 \ldots j_n} - \tilde{a}_{j_1 \ldots j_n}) x_1^{j_1} \ldots x_{n-2}^{j_{n-2}} = 0$$

su visais j_{n-1}, j_n.

Pakartoję samprotavimą n kartų, matome, kad (7.10) lygybė teisinga tik tada, kai

$$a_{j_1 \ldots j_n} - \tilde{a}_{j_1 \ldots j_n} = 0$$

su visais $j_1, \ldots, j_n$.

Antroji teoremos dalis įrodyta.

n kintamųjų polinomo f (7.8) išraiška vadinama *jo normaliuoju pavidalu.* Dėmuo

$$a_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n}$$

vadinamas *polinomo nariu.* Suma $j_1 + \ldots + j_n$ vadinama *to nario laipsniu.* Žiedo $\mathbf{Z}$ elementas $a_{j_1 \ldots j_n}$ vadinamas to nario *koeficientu.* $\max(j_1 + \ldots + j_n)$ tų $j_1, j_2, \ldots, j_n$, su kuriais $a_{j_1 \ldots j_n} \neq 0$, vadinamas *polinomo f laipsniu* ir žymimas $\deg(f)$.

Kiekvieno polinomo laipsnis nustatomas vienareikšmiškai.

Pavyzdys. Polinomo

$$g(x, y, z) = (x+1)\, y - 6y^3 z + 8xyz^5$$

normalusis pavidalas yra

$$g(x, y, z) = y + xy - 6y^3 z - 8xyz^5.$$

Polinomo nariai yra y, xy, $-6y^3z$, $8xyz^5$, jų koeficientai atitinkamai $-$ 1, 1, -6, 8. Nario y laipsnis yra $0+1+0=1$, nario xy $-$ $1+1+0=2$, nario $-6y^3z$ $-$ $0+3+1=4$ ir nario $8xyz^5$ laipsnis yra $1+1+5=7$. Taigi tas polinomas yra trijų kintamųjų septintojo laipsnio polinomas virš $\mathbf{Z}$.

133 teoremos antrojoje dalyje įrodėme, kad *du normaliojo pavidalo n kintamųjų polinomai yra lygūs tada ir tik tada, kai jų atitinkamų narių koeficientai lygūs.* (Atitinkami nariai yra $ax_1^{j_1} \ldots x_n^{j_n}$ ir $bx_1^{j_1} \ldots x_n^{j_n}$.)

Iš (7.9) gauname šitokias sudėties ir atimties taisykles.

Sudedant normaliojo pavidalo polinomus, reikia sudėti jų atitinkamų narių koeficientus, o atimant – atimti atitinkamų narių koeficientus.

Taigi polinomų sumos (skirtumo) laipsnis ne didesnis už dėmenų (turinio ir atėminio) laipsnius.

Aiškinsimės, kaip dauginami normaliojo pavidalo polinomai.

134 teorema. *Jeigu*

$$f(x_1, \ldots, x_n) = \sum_{j_1 \ldots j_n} a_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n},$$

$$g(x_1, \ldots, x_n) = \sum_{l_1 \ldots l_n} b_{l_1 \ldots l_n} x_1^{l_1} \ldots x_n^{l_n},$$

tai

$$f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n) = \sum_{k_1 \ldots k_n} c_{k_1 \ldots k_n} x_1^{k_1} \ldots x_n^{k_n};$$

čia

$$c_{k_1 \ldots k_n} = \sum_{\substack{j_1+l_1=k_1 \\ \cdots\cdots\cdots \\ j_n+l_n=k_n}} a_{j_1 \ldots j_n} b_{l_1 \ldots l_n}.$$

Įrodymas. Taikysime matematinės indukcijos metodą. Kai $n=1$, teoremos tvirtinimas yra teisingas pagal vieno kintamojo polinomų daugybos taisyklę.

Tarkime, kad teorema teisinga, kai $n=r$.

Įrodysime, kad ji teisinga ir kai $n=r+1$. Dauginame polinomus

$$f(x_1, \ldots, x_{r+1}) = \sum_j f_j(x_1, \ldots, x_r)\, x_{r+1}^j,\ g(x_1, \ldots, x_{r+1}) =$$

$$= \sum_l g_l(x_1, \ldots, x_r)\, x_{r+1}^l$$

ir gauname

$$f(x_1, \ldots, x_{r+1}) \cdot g(x_1, \ldots, x_{r+1}) =$$

$$= \sum_k \left(\sum_{j+l=k} f_j(x_1, \ldots, x_r)\, g_l(x_1, \ldots, x_r) \right) x_{r+1}^k.$$

Jeigu

$$f_j(x_1, \ldots, x_r) = \sum_{j_1 \ldots j_r} a^{(j)}_{j_1 \ldots j_r} x_1^{j_1} \ldots x_r^{j_r},$$

$$g_l(x_1, \ldots, x_r) = \sum_{l_1 \ldots l_r} b^{(l)}_{l_1 \ldots l_r} x_1^{l_1} \ldots x_r^{l_r},$$

tai pagal prielaidą

$$f_j(x_1, \ldots, x_r)\, g_l(x_1, \ldots, x_r) = \sum_{k_1 \ldots k_r} \left(\sum_{\substack{j_1+l_1=k_1 \\ \cdots\cdots\cdots \\ j_r+l_r=k_r}} a^{(j)}_{j_1 \ldots j_r} b^{(l)}_{l_1 \ldots l_r} \right) x_1^{k_1} \ldots x_r^{k_r}.$$

Iš tų išraiškų išplaukia

$$f(x_1, \ldots, x_{r+1})\, g(x_1, \ldots, x_{r+1}) =$$

$$= \sum_k \left(\sum_{j+l=k} \left(\sum_{k_1 \ldots k_r} \sum_{\substack{j_1+l_1=k_1 \\ \cdots\cdots\cdots \\ j_r+l_r=k_r}} a^{(j)}_{j_1 \ldots j_r} b^{(l)}_{l_1 \ldots l_r} \right) x_1^{k_1} \ldots x_r^{k_r} \right) x_{r+1}^k =$$

$$= \sum_{k_1 \ldots k_r k} \left(\sum_{\substack{j_1+l_1=k_1 \\ \cdots\cdots\cdots \\ j_r+l_r=k_r \\ j+l=k}} a^{(j)}_{j_1 \ldots j_r} b^{(l)}_{l_1 \ldots l_r} \right) x_1^{k_1} \ldots x_r^{k_r} x_{r+1}^k.$$

Taigi tarę, kad teorema teisinga, kai $n=r$, įsitikiname, jog ji teisinga ir kai $n=r+1$. Todėl teorema teisinga su kiekvienu $n \geqslant 1$.

Išvada. *Polinomų f ir g sandaugos laipsnis lygus dauginamųjų laipsnių sumai.*

Tarkime, kad

$$\deg(f)=\max(j_1+\ldots+j_n)=s_1+\ldots+s_n,$$
$$\deg(g)=\max(l_1+\ldots+l_n)=m_1+\ldots+m_n.$$

Polinomas g turės narį $ax_1^{m_1}\ldots x_n^{m_n}$, o polinomas f turės narį $bx_1^{s_1}\ldots x_n^{s_n}$. Kadangi

$$\max(k_1+\ldots+k_n)=\max(j_1+\ldots+j_n)+\max(l_1+\ldots+l_n)=$$
$$=(s_1+\ldots+s_n)+(m_1+\ldots+m_n),$$

o sandaugos fg nario

$$Ax_1^{s_1+m_1}\ldots x_n^{s_n+m_n}$$

koeficientas yra $A=ba\neq O$ ($\check{\mathbf{Z}}$ neturi nulio daliklių), tai $\deg(fg)=\deg(f)+\deg(g)$.

Teoremos esmę galima išreikšti šitokia taisykle.

Dauginant du n kintamųjų polinomus, pirmojo polinomo kiekvieną narį reikia padauginti iš antrojo polinomo kiekvieno nario ir gautąsias sandaugas sudėti sutraukus panašiuosius narius.

Panašiaisiais nariais vadinami nariai $ax_1^{j_1}\ldots x_n^{j_n}$ ir $bx_1^{j_1}\ldots x_n^{j_n}$. Sutraukti panašiuosius narius – reiškia sudėti jų koeficientus.

Uždaviniai

13. Nustatykite šių polinomų laipsnius, taip pat jų laipsnius kintamojo x_i atžvilgiu, $i=1, 2, \ldots, n$:

a) $4-6x_1^3x_2+19x_1x_2^3-6x_1^2x_2^2+7x_1^3x_2^3$;

b) $3x_1x_2+5x_1x_2x_3-9x_1^5x_3^2-11x_2^4x_3^3-3x_1^2x_2^3x_3^4$;

c) $x_1^3-6x_1^3x_2^5+6x_1x_2x_3^5+6x_2x_3x_4^2-8x_1x_2x_3^3x_4^3-13x_4^5+11$.

14. Šiuos polinomus užrašykite kaip polinomus virš $\mathbf{Q}[x_1]$ ir kaip polinomus virš $\mathbf{Q}[x_2]$:

a) $15-6x_1x_2^3+7x_1^2x_2^3+5x_1x_2-6x_1^2x_2^3-7x_1^2x_2+x_1^3x_2^3+x_1^3x_2$;

b) $3x_1x_2-7x_1^3x_2-9x_1^2x_2^2+17x_1^3x_2^2+11x_1^3x_2^3+35-14x_1^4x_2$.

15. Šiuos polinomus užrašykite kaip polinomus virš $\mathbf{Z}[x_1, x_2]$, kaip polinomus virš $\mathbf{Z}[x_1, x_3]$ ir kaip polinomus virš $\mathbf{Z}[x_2, x_3]$:

a) $x_1x_2x_3-2x_1x_2x_3^2+4x_1^2x_2x_3+6x_1^2x_2^2x_3^3-7x_1x_2^2x_3^2$;

b) $3+3x_1^2x_3^3-5x_1x_2^4+4x_1^3x_2x_3^2+13x_1x_2^2x_3^5-4x_1x_2^2x_3^4+4x_1x_2x_3+2x_1^2x_2^2x_3^2-18x_1^3x_2^2x_3^2$.

16. Apskaičiuokite $f+g$, $f-g$, fg:

a) $f=15-x_1x_2+3x_1x_2x_3^4-6x_1^2x_2x_3^4+8x_2^3x_3^4-17x_1x_2x_3$,
$g=65x_1x_2-29x_1x_2x_3^4+17x_1x_2x_3-11x_2^2x_3^2-7x_2^3x_3^4+23$;

b) $f=x_1x_2x_3x_4-6x_1^3x_4+5x_1x_2x_3^3+3x_2^2x_4^5-7x_2x_3^3x_4^5$,
$g=3-4x_1x_2x_3x_4+9x_1x_2x_3^3-7x_1^3x_4+8x_2^2x_4^5-13x_1x_2x_3^4x_4^5$.

§65. Kelių kintamųjų polinomų žiedo konstravimas

Nuosekliai konstruodami žiedus $\check{Z}[x_1]$, $\check{Z}[x_1, x_2]$, ..., $\check{Z}[x_1, \ldots, x_n]$, sudarėme n kintamųjų polinomų virš integralumo srities $\check{Z}$ (su vienetu $e\neq O$) žiedą $\check{Z}[x_1, \ldots, x_n]$. Paėmę elementų $x_1, \ldots, x_n$ bet kurį kėlinį $x_{i_1}, \ldots, x_{i_n}$, galime sudaryti žiedą $\check{Z}[x_{i_1}, \ldots, x_{i_n}]$. Kuo jis skirsis nuo žiedo $\check{Z}[x_1, \ldots, x_n]$? Kadangi $x_1, \ldots, x_n$ yra transcendetiniai elementai $\check{Z}$ atžvilgiu, tai ir x_{i_1} transcendentinis $\check{Z}$ atžvilgiu. Tačiau neaišku, ar elementas x_{i_2} transcendentinis $\check{Z}[x_{i_1}]$ atžvilgiu. Ir apskritai neaišku, ar x_{i_s} transcendentinis $\check{Z}[x_{i_1}, \ldots, x_{i_{s-1}}]$ atžvilgiu.

135 teorema. *Kiekvienas* x_i $(1\leqslant i\leqslant n)$, *transcendentinis* $\check{Z}[x_1, \ldots, x_{i-1}]$ *atžvilgiu, yra transcendentinis ir* $\check{Z}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ *atžvilgiu. Imant kiekvieną elementų* $x_1, \ldots, x_n$ *kėlinį* $x_{i_1}, \ldots, x_{i_n}$, *žiedai* $\check{Z}[x_1, \ldots, x_n]$ *ir* $\check{Z}[x_{i_1}, \ldots, x_{i_n}]$ *sutampa.*

Įrodymas. Nagrinėkime lygybę

$$\sum_{j_i} f_{j_i}x_i^{j_i}=0,$$

kurioje

$$f_{j_i}\in\check{Z}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n].$$

Pagal (7.8)

$$f_{j_i}=\sum_{j_1\ldots j_{i-1}j_{i+1}\ldots j_n} a^{(j_i)}_{j_1\ldots j_{i-1}j_{i+1}\ldots j_n}x_1^{j_1}\ldots x_{i-1}^{j_{i-1}}x_{i+1}^{j_{i+1}}\ldots x_n^{j_n}. \qquad (7.11)$$

Todėl

$$\sum_{j_i} f_{j_i}x_i^{j_i}=\sum_{j_i}\left(\sum_{j_1\ldots j_{i-1}j_{i+1}\ldots j_n} a^{(j_i)}_{j_1\ldots j_{i-1}j_{i+1}\ldots j_n}x_1^{j_1}\ldots x_{i-1}^{j_{i-1}}x_{i+1}^{j_{i+1}}\ldots x_n^{j_n}\right)x_i^{j_i}=$$

$$=\sum_{j_1\ldots j_n} a^{(j_i)}_{j_1\ldots j_{i-1}j_{i+1}\ldots j_n}x_1^{j_1}\ldots x_n^{j_n}=0.$$

Įrodėme (žr. 133 teoremos antrosios dalies įrodymą), kad iš pastarosios lygybės išplaukia lygybės

$$a^{(j_i)}_{j_1\ldots j_{i-1}j_{i+1}\ldots j_n}=O$$

su visais $j_1, \ldots, j_n$. Remdamiesi tomis lygybėmis, iš (7.11) gauname lygybes

$$f_{j_i} = O \quad (j = 0, 1, \ldots).$$

Taigi iš lygybės

$$\sum_{j_i} f_{j_i} x_i^{j_i} = O$$

išplaukia, kad $f_{j_i} = O$ su visais $j_i \geqslant 0$.

Taigi įrodėme, kad x_i yra transcendentinis elementas $\check{\mathbf{Z}}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ atžvilgiu. Juo labiau x_i yra transcendentinis $\check{\mathbf{Z}}[x_{j_1}, \ldots, x_{j_{i-1}}]$ atžvilgiu, kai $j_1, \ldots, j_{i-1}$ yra aibės $1, \ldots, i-1, i+1, \ldots, n$ bet kuris gretinys iš $i-1$ elemento. Taigi imant bet kurį skaičių $1, 2, \ldots, n$ kėlinį $i_1, \ldots, i_n$, polinomų žiedas $\check{\mathbf{Z}}[x_{i_1}, \ldots, x_{i_n}]$ egzistuoja ir yra vienintelis izomorfizmo tikslumu. Jo elementai šitokio pavidalo:

$$\sum_{j_1 \ldots j_n} a_{j_1 \ldots j_n} x_{i_1}^{j_1} \ldots x_{i_n}^{j_n}.$$

Kadangi daugyba komutatyvi, tai ta suma priklauso žiedui $\check{\mathbf{Z}}[x_1, \ldots, x_n]$, nes sukeitę dauginamuosius vietomis gausime (7.8) išraiškos sumą. Be to, kiekviena (7.8) išraiškos suma yra $\check{\mathbf{Z}}[x_{i_1}, \ldots, x_{i_n}]$ elementas dėl tų pačių priežasčių. Taigi

$$\check{Z}[x_{i_1}, \ldots, x_{i_n}] \subset \check{Z}[x_1, \ldots, x_n] \subset \check{Z}[x_{i_1}, \ldots, x_{i_n}].$$

Šie sąryšiai rodo, kad žiedai sutampa.

Kaip ir vieno kintamojo polinomas, n kintamųjų polinomas

$$f(x_1, \ldots, x_n) = \sum_{j_1 \ldots j_n} a_{j_1 \ldots j_n} x_1^{j_1} \ldots x_n^{j_n}$$

apibrėžia funkciją

$$f\colon (Z')^n \to Z'$$

šitokiu būdu:

$$\big(\forall (z_1, \ldots, z_n) \in (Z')^n\big) f(z_1, \ldots, z_n) = \sum_{j_1 \ldots j_n} a_{j_1 \ldots j_n} z_1^{j_1} \ldots z_n^{j_n};$$

čia $\mathbf{Z}'$ – bet koks žiedo $\check{\mathbf{Z}}$ plėtinys.

Funkcija f vadinama polinomine n kintamųjų funkcija ir žymima $f(z_1, \ldots, z_n)$. Jos reikšmė taške $(z_1, \ldots, z_n) = (l_1, \ldots, l_n)$

$$f(l_1, \ldots, l_n) = \sum_{j_1 \ldots j_n} a_{j_1 \ldots j_n} l_1^{j_1} \ldots l_n^{j_n}$$

vadinama (pagal tradiciją) *polinomo f reikšme taške $(l_1, \ldots, l_n)$.*

Jeigu polinomai f ir g iš $\check{Z}[x_1, \ldots, x_n]$ yra lygūs, tai atitinkamos polinominės funkcijos srityje $(Z')^n$ irgi lygios:

$$(\forall (l_1, \ldots, l_n) \in (Z')^n)\ f(l_1, \ldots, l_n) = g(l_1, \ldots, l_n),$$

t. y. polinomų reikšmės lygios ir aibėje $(\check{Z})^n$, nes

$$(\check{Z})^n \subset (Z')^n.$$

Atvirkščias teiginys ne visada teisingas. Tuo įtikina 61 paragrafo pavyzdys, kuriame dviejų nelygių vieno kintamojo polinomų virš lauko $\mathbf{L}_p$ polinominės funkcijos lygios.

§66. Dalumo sąryšis polinomų virš integralumo srities žieduose

Įvairūs polinomų teorijos klausimai nagrinėjami naudojantis polinomų dalumo sąryšiu. Šiame paragrafe aptarsime dalumo sąryšio savybes polinomų (n kintamųjų, $n \geqslant 1$) virš integralumo srities žieduose.

Sakoma, kad polinomas $f \in \check{Z}[x_1, \ldots, x_n]$ dalijasi iš polinomo $g \neq O$, $g \in \check{Z}[x_1, \ldots, x_n]$, jei egzistuoja toks polinomas $q \in \check{Z}[x_1, \ldots, x_n]$, su kuriuo teisinga lygybė $f = gq$. Rašoma $g \mid f$.

Tuo atveju polinomas g *vadinamas polinomo f dalikliu*, o polinomas f – *polinomo g kartotiniu.* Polinomas q vadinamas *polinomų f ir g santykiu*, arba *papildomuoju dalikliu.*

Pavyzdys. Polinomas $g(x_1, x_2, x_3) = x_1^2 + 2x_1x_2 - x_3^2$ yra polinomo $f(x_1, x_2, x_3) = x_1^3x_2x_3 + 2x_1^2x_2^2x_3 - x_1x_2x_3^3 - x_1^2 - 2x_1x_2 + x_3^2$ daliklis, nes $f(x_1, x_2, x_3) = (x_1^2 + 2x_1x_2 - x_3^2) \times (x_1x_2x_3 - 1)$. Taigi $q(x_1, x_2, x_3) = x_1x_2x_3 - 1$.

Kadangi n kintamųjų ($n \geqslant 1$) polinomų virš integralumo srities žiedas yra integralumo sritis su vienetu, tai dalumo sąryšio tame žiede visos savybės analogiškos atitinkamoms jo savybėms integralumo srityje su vienetu (žr. § 51). Atkreipsime dėmesį į štai ką: *jeigu $g \mid f$, tai polinomas q, tenkinantis lygybę $f = gq$, nustatomas vienareikšmiškai* (94 teorema).

Polinomų žiedo $\check{Z}[x_1, \ldots, x_n]$ vieneto dalikliai sutampa su integralumo srities $\check{Z}$ vieneto dalikliais.

Du polinomai $f(x_1, \ldots, x_n)$ ir $g(x_1, \ldots, x_n)$ vadinami asocijuotaisiais, kai yra toks integralumo srities $\check{Z}$ vieneto daliklis ε, su kuriuo teisinga lygybė

$$g(x_1, \ldots, x_n) = \varepsilon f(x_1, \ldots, x_n).$$

Asocijuotųjų polinomų laipsniai lygūs.

Dabar išvardysime dalumo sąryšio savybes.

1. *Kiekvienas polinomas* $f(x_1, \ldots, x_n)$ *dalijasi iš integralumo srities vieneto kiekvieno daliklio.*

2. *Kiekvienas nenulinis polinomas* $f(x_1, \ldots, x_n)$ *dalijasi iš kiekvieno sau asocijuoto polinomo* $\varepsilon f(x_1, \ldots, x_n)$.

3. *Nulinis polinomas* $O(x)$ *dalijasi iš kiekvieno nenulinio polinomo.*

4. *Jeigu* $g \mid f$, *tai su bet kokiais vieneto dalikliais* ε_1 *ir* ε_2 $\varepsilon_1 g \mid \varepsilon_2 f$.

5. *Jeigu* $g \mid f$ *ir* $h \mid g$, *tai* $h \mid f$.

6. *Jeigu* $g \mid f$ *ir* h *— bet koks nenulinis polinomas, tai* $gh \mid hf$.

7. *Jeigu* $g \mid f$, *tai su bet kokiu polinomu* h $g \mid hf$.

8. *Jeigu* $g \mid f_1$ *ir* $g \mid f_2$, *tai* $g \mid f_1 \pm f_2$.

Iš 7 ir 8 savybių matematinės indukcijos metodu gaunamas šitoks teiginys: *jeigu* $g \mid f_j$, $j=1, 2, \ldots, n$, o h_j, $j=1, 2, \ldots, n$ *— bet kokie polinomai, tai*

$$g \mid \sum_{j=1}^{n} h_j f_j.$$

9. *Jeigu* $g_1 \mid f_1$ *ir* $g_2 \mid f_2$, *tai* $g_1 g_2 \mid f_1 f_2$.

Ši savybė matematinės indukcijos metodu apibendrinama šitaip: *jeigu* $gf \mid f_j$, $j=1, 2, \ldots, n$, *tai*

$$\prod_{j=1}^{n} g_j \mid \prod_{j=1}^{n} f_j.$$

10. *Jeigu* $g \mid f$, *tai su kiekvienu natūriniu* $ng^n \mid f^n$.

Ši savybė yra apibendrintos 9 savybės išvada.

11. *Jeigu* $g \mid f$ *ir* $f \mid g$, *tai* f *ir* g *yra asocijuotieji polinomai.*

Polinomo f *daliklis, kurio laipsnis lygus nuliui arba sutampa su polinomo* f *laipsniu, vadinamas trivialiuoju dalikliu.*

Aišku, kad *vieneto dalikliai yra kiekvieno polinomo trivialieji dalikliai. Nenulinio polinomo asocijuotieji polinomai yra to polinomo trivialieji dalikliai.*

Polinomo netrivialieji dalikliai dar vadinami tiesioginiais dalikliais.

Akivaizdus toks teiginys: *jeigu* $g \mid f$, *tai* $0 \leqslant \deg(g) \leqslant \deg(f)$. *Jeigu* g *yra polinomo* f *tiesioginis daliklis, tai* $0 < \deg(g) < \deg(f)$.

Jeigu polinomas f_1 yra polinomo f tiesioginis daliklis, f_2 — polinomo f_1 tiesioginis daliklis, ..., f_{j+1} — polinomo f_j tiesioginis daliklis, tai *polinomų* $f_1, f_2, \ldots, f_j, f_{j+1} \ldots$ *seka vadinama polinomo* f *tiesioginių daliklių seka.*

---

136 teorema. *Polinomo tiesioginių daliklių seka yra baigtinė.*

Įrodymas. Pakanka nagrinėti polinomus f, kurių $\deg(f)\geqslant 2$. Sakykime, $f_0=f$ ir $f_{j+1}\mid f_j, j=0, 1, 2, \ldots, f_1, f_2, \ldots, f_k, f_{k+1}$ – polinomo f tiesioginių daliklių seka, o $\deg(f)=m$. Pažymėkime $\deg(f_j)=m_j$.

Natūrinių skaičių seka $\{m_j\}$ yra mažėjanti, nes $m>m_1>m_2>\ldots>m_j>m_{j+1}>\ldots\geqslant 1$. Tokia seka yra baigtinė ir turi ne daugiau kaip $m-1$ narį.

Imkime bet kurį nenulinį polinomą $g\in\check{Z}[x_1, \ldots, x_n]$. Tarkime, kad $\check{Z}_g[x_1, \ldots, x_n]$ yra aibė polinomų iš $\check{Z}[x_1, \ldots, x_n]$, kurie dalijasi iš polinomo g. Iš 7 ir 8 savybių išplaukia, kad ta aibė turi idealo apibrėžime išvardytas savybes (žr. § 52). Todėl teisingas šitoks teiginys.

Nelygaus nuliui n kintamųjų polinomo g kartotinių aibė $\check{Z}_g[x_1, \ldots, x_n]$ yra polinomų žiedo $\check{Z}[x_1, \ldots, x_n]$ vyriausiasis idealas; jį žymėsime (g).

Paėmę $n=1$, gauname vieno kintamojo polinomų virš $\check{Z}$ vyriausiąjį idealą

$$(g)=\check{Z}_g[x]=\{g(x)f(x)\mid f(x)\in\check{Z}[x]\}.$$

§67. Hornerio schema

66 paragrafe įsitikinome, kad polinomų virš integralumo srities dalumo savybės analogiškos sveikųjų skaičių dalumo savybėms. Tačiau ne visos sveikųjų skaičių žiedo savybės turi savo analogus polinomų žiede $\check{Z}[x]$, kai $\check{Z}$ – integralumo sritis. Pavyzdžiui, polinomų virš integralumo srities žiede nėra teisinga teorema, analogiška dalybos su liekana sveikųjų skaičių žiede teoremai. Įrodysime, kad vieno kintamojo polinomų virš integralumo srities žiede galima dalyba su liekana iš specialaus pirmojo laipsnio polinomo; aiškinsime algoritmą nepilnojo dalmens koeficientams ir liekanai rasti. Tą metodą vadinsime Hornerio schema (V. G. Horner, 1786–1837, anglų matematikas).

137 (polinomo dalybos su liekana iš dvinario) teorema. *Jeigu $f(x)$ yra n-ojo laipsnio polinomas virš integralumo srities $\check{Z}$, tai su kiekvienu $l\in\check{Z}$ egzistuoja vienintelis $n-1$-ojo laipsnio polinomas $g(x)\in\check{Z}[x]$ ir vienintelė liekana $r\in\check{Z}$, su kuriais teisinga lygybė $f(x)=(x-l)g(x)+r$.*

Įrodymas. Kadangi $o(x)=(x-l)o(x)+O$, tai pakanka įrodyti teoremą, kai $n\geqslant 1$.

Kaip žinome, dauginant polinomus, jų laipsniai sudedami, o $\deg(x-l)=1$. Kad būtų teisinga lygybė $f(x)=(x-l)g(x)+r$, turi būti $\deg(g)=\deg(f)-1=n-1$.

Tarkime, kad $f(x)=\sum_{j=0}^{n} a_j x^j$. Pažymėkime $g(x)=\sum_{j=0}^{n-1} b_j x^j$ ir raskime tokius $b_0, b_1, \ldots, b_{n-1}$ ir r, kad būtų teisinga teoremos lygybė.

Kadangi

$$(x-l)g(x)+r=b_{n-1}x^n+(b_{n-2}-lb_{n-1})x^{n-1}+(b_{n-3}-lb_{n-2})x^{n-2}+$$
$$+\ldots+(b_2-lb_3)x^3+(b_1-lb_2)x^2+(b_0-lb_1)x+(r-lb_0),$$

tai iš polinomų lygybės gauname tiesinių lygčių sistemą

$$\begin{aligned}
b_{n-1} \qquad\qquad\qquad\qquad &= a_n, \\
-lb_{n-1}+b_{n-2} \qquad\qquad &= a_{n-1}, \\
-lb_{n-2}+b_{n-3} \qquad &= a_{n-2}, \\
\dots\dots\dots\dots\dots\dots\dots\dots&\dots\dots \\
-lb_2+b_1 \qquad &= a_2, \\
-lb_1+b_0 \quad &= a_1, \\
-lb_0+r &= a_0,
\end{aligned}$$

kurioje yra $n+1$ lygtis ir $n+1$ kintamasis $b_{n-1}, \dots, b_1, b_0, r$. Tos sistemos matrica yra

$$A=\begin{pmatrix} e & 0 & 0 & \dots & 0 & 0 \\ -l & e & 0 & \dots & 0 & 0 \\ 0 & -l & e & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & e & 0 \\ 0 & 0 & 0 & \dots & -l & e \end{pmatrix}.$$

Kadangi $|A|=e\neq O$, tai sistema turi vienintelį sprendinį ir jo komponentės priklauso integralumo sričiai Ž. (Tuo įsitikinsime ieškodami sistemos sprendinio.) Taigi teorema įrodyta.

Išsprendę šią sistemą, gausime $b_{n-1}=a_n$, $b_{n-2}=a_{n-1}+lb_{n-1}$, $\dots, b_1=$ $=a_2+lb_2$, $b_0=a_1+lb_1$, $r=a_0+lb_0$. Vadinasi, polinomo $g(x)$ koeficientus ir liekaną galima apskaičiuoti iš šitokių rekurentinių formulių:

$$b_{n-1}=a_n,\ b_{n-(k+1)}=a_{n-k}+lb_{n-k},\quad k=1,\ 2,\ \dots,\ n-1,$$

$$r=a_0+lb_0.$$

Skaičiavimas pagal šias formules vadinamas Hornerio schema. Skaičiavimo rezultatus patogu užrašyti vadinamąja Hornerio lentele:

	a_n	a_{n-1}	a_{n-2}	...	a_2	a_1	a_0
l	b_{n-1}	b_{n-2}	b_{n-3}	...	b_1	b_0	r

Pirmojoje lentelės eilutėje, pradėdami nuo vyriausiojo, eilės tvarka surašome $f(x)$ koeficientus. Antrojoje eilutėje prieš pirmąjį stulpelį užrašome elementą l. Pirmajame stulpelyje įrašome elementą a_n, nes $b_{n-1}=a_n$. $k+1$-ojo ($k=1, \dots, n-1$) stulpelio elementą apskaičiuojame pagal nurodytas formules.

Pavyzdys. Rasime polinomus $g(x)$ ir liekanas r, kai $f(x)=3x^7-5x^5+6x^4-2x^2+3x-1$ ir a) $l=2$, b) $l=-2$.

a) Sudarome Hornerio lentelę

	3	0	−5	6	0	−2	3	−1
2	3	6	7	20	40	78	159	317

Šiuo atveju

$$g(x)=3x^6+6x^5+7x^4+20x^3+40x^2+78x+159, \quad r=317.$$

b) Hornerio lentelė:

	3	0	−5	6	0	−2	3	−1
−2	3	−6	7	−8	16	−34	71	−143

Šiuo atveju

$$g(x)=3x^6-6x^5+7x^4-8x^3+16x^2-34x+71, \quad r=-143.$$

Taigi

$$f(x)=(x-2)(3x^6+6x^5+7x^4+20x^3+40x^2+78x+159)+317=$$
$$=(x+2)(3x^6-6x^5+7x^4-8x^3+16x^2-34x+71)-143.$$

138 (polinomo skleidimo dvinario laipsniais) teorema. *Jeigu $f(x)$ yra n-ojo laipsnio polinomas virš integralumo srities, o l – bet koks tos srities elementas, tai polinomą $f(x)$ vieninteliu būdu galima išreikšti šitaip*:

$$f(x)=\sum_{j=0}^{n} r_j(x-l)^j$$

su tos srities elementais r_j $(j=0, 1, \ldots, n)$.

Gautąją išraišką vadiname *polinomo $f(x)$ skleidiniu dvinario $x-l$ laipsniais.*

Įrodymas. Pagal dalybos iš dvinario $x-l$ teoremą

$$(1)\ f(x)=(x-l)f_1(x)+r_0, \quad \deg(f_1)=n-1,$$
$$(2)\ f_1(x)=(x-l)f_2(x)+r_1, \quad \deg(f_2)=n-2,$$
$$(3)\ f_2(x)=(x-l)f_3(x)+r_2, \quad \deg(f_3)=n-3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(n)f_{n-1}(x)=(x-l)f_n(x)+r_{n-1}, \quad \deg(f_n)=n-n=0,$$
$$(n+1)\ f_n(x)=r_n.$$

Šiose lygybėse polinomai $f_k(x)$, $k=1, 2, \ldots, n-1$, ir liekanos r_j, $j=0, 1, \ldots, n$, nustatomos vienareikšmiškai. Įrašę vietoje $f_k(x)$ jo išraišką iš $k+1$ lygybės, $k=1, 2, \ldots, n$, gausime

$$f(x)=r_n\cdot(x-l)^n+r_{n-1}\cdot(x-l)^{n-1}+\ldots+r_2\cdot(x-l)^2+r_1\cdot(x-l)+r_0.$$

Praktiškai polinomo skleidinį dvinario $x-l$ laipsniais gausime nuosekliai dalydami iš dvinario $x-l$ su liekana. Tai patogiausia atlikti naudojantis Hornerio schema.

Pavyzdys. Polinomą $f(x)=3x^6+5x^5-6x^4+2x^2-1$ išreikšime $x-2$ laipsniais. Nuosekliai dalijame iš dvinario $x-2$ pagal Hornerio schemą:

a	3	5	-6	0	2	0	-1
2	3	11	16	32	66	132	$263=r_0$
2	3	17	50	132	330	$792=r_1$	
2	3	25	100	232	$994=r_2$		
2	3	31	162	$656=r_3$			
2	3	37	$236=r_4$				
2	3	$43=r_5$					
2	$3=r_6$						

Gauname

$$f(x)=3(x-2)^6+43(x-2)^5+236(x-2)^4+656(x-2)^3+994(x-2)^2+792(x-2)+263.$$

Iš lygybės

$$f(x)=(x-l)\,q(x)+r$$

išplaukia, kad kairiojoje pusėje esančio polinomo reikšmės yra lygios dešiniojoje pusėje esančio polinomo atitinkamoms reikšmėms. Kai $x=l$, $O\cdot q(l)=O$, gauname lygybę $f(l)=r$. Taigi įrodėme teoremą, vadinamą prancūzų matematiko *Bezu* vardu (E. Bezout, 1730–1783).

Bezu teorema. *Liekana, gauta dalijant polinomą $f(x)$ iš polinomo $x-l$, lygi polinomo $f(x)$ reikšmei taške l.*

Pavyzdys. Kai $f(x)=3x^7-5x^5+6x^4-2x^2+3x-1$, iš pavyzdžio (žr. 250–251 p.) ir Bezu teoremos gauname $f(2)=317$, o $f(-2)=-143$.

Kai žinomi polinomo f koeficientai ir integralumo srities $\check{Z}$ elementas l, polinomo reikšmę $f(l)$ nesunku rasti naudojantis Hornerio lentele. *Antrosios eilutės paskutiniajame langelyje esantis elementas ir yra polinomo reikšmė taške l.*

Pavyzdys. Rasime polinomo $f(x)=6x^5+(3+i)x^3+(7+2i)x-14$ reikšmę taške $l=1-i$.

Užpildome Hornerio lentelę

	6	0	$3+i$	0	$7+2i$	-14
$1-i$	6	$6-6i$	$3-11i$	$-8-14i$	$-15-4i$	$-33+11i$

ir gauname $f(1-i)=-33+11i$.

Hornerio schema labai paprasta, lengvai įsimenama. Patartina mokyti ja naudotis ir vyresniųjų klasių mokinius.

Uždaviniai

17. Raskite tokį polinomą (nepilnąjį dalmenį) $q(x)$ ir liekaną r, kad būtų $f(x)=(x-l)q(x)+r$, kai:

a) $f(x)=3x+2$, $l=5$;
b) $f(x)=16x^2-5x+3$, $l=2$;
c) $f(x)=3x^2+4x-5$, $l=-2$;
d) $f(x)=x^3-4x^3+16x^2-7x+1$, $l_1=1$, $l_2=-1$;
e) $f(x)=16x^8-13x^7+4x^5-3x^3+6x^2+3$, $l_1=2$, $l_2=-3$;
f) $f(x)=4x^5-6x^4+3x^3-6$, $l_1=i$, $l_2=-i$;
g) $f(x)=-6x^7-3x^5+5x^4+3x^2+18$, $l_1=1$, $l_2=-1$.

18. Apskaičiuokite polinomo $f(x)$ reikšmę taške l; polinomą $f(x)$ išskleiskite dvinario $x-l$ laipsniais, kai:

a) $f(x)=2-6x^4+3x-5x^2$, $l=1$;
b) $f(x)=14x-5+3x^5-6x^6$, $l_1=2$, $l_2=-2$;
c) $f(x)=14x^6+5x^5+3x^4+6x-10$, $l_1=1$, $l_2=3$, $l_2=-3$;
d) $f(x)=7x^3+7x^6-8x^4+3x^2-14$, $l_1=i$, $l_2=-i$.

§68. Vieno kintamojo polinomų šaknys

Polinomo $f(x)\in\check{Z}[x]$ šaknimi vadinamas integralumo srities $\check{Z}$ arba bet kurio jos plėtinio Z' elementas l, su kuriuo

$$f(l)=O.$$

Polinomo šaknis yra toks $\check{Z}$ arba Z' elementas, kurį polinominė funkcija $f(z)$ atvaizduoja į nulį (nulinį $\check{Z}$ elementą).

Jeigu $f(x)=O$ (x), tai su kiekvienu $z\in Z^1$ gauname $f(z)=O$. Taigi nulinio polinomo šaknys yra visi $\check{Z}$ ir jo plėtinio Z' elementai. Nulinio laipsnio nelygus nuliui polinomas visai neturi šaknų, nes su kiekvienu $z\in Z'$ $f(z)=c\neq O$.

Iš apibrėžimo išplaukia, kad polinomo $f(x)$ virš $\check{Z}$ šaknis yra kiekvienas aibės $\{l \mid f(l)=O,\ l\in Z'\}$ elementas, t. y. lygties

$$f(z)=O$$

kiekvienas sprendinys. (Šiuo atveju $f(z)=O$ yra ne polinomų lygybė, o vienvietis predikatas, kuris tampa teisingu teiginiu su tomis reikšmėmis $z=l$,

su kuriomis $f(l)=O$. Su visomis kitomis z reikšmėmis jis tampa neteisingu teiginiu.) Dažnai *lygties* $f(z)=O$ *sprendiniai vadinami tos lygties šaknimis.*

139 teorema. *l yra polinomo* $f(x)$ *šaknis tada ir tik tada, kai* $f(x)$ *dalijasi iš* $x-l$, *t. y.* $f(x)=(x-l)q(x)$.

Įrodymas. Iš Bezu teoremos išplaukia

$$f(x)=(x-l)\,q(x)+f(l).$$

Jeigu $f(l)=O$, tai $r=O$ ir $(x-l)\mid f(x)$. Sąlyga būtina.
Jeigu $(x-l)\mid f(x)$, tai $f(x)=(x-l)\,q(x)$ ir $f(l)=(l-l)\,q(l)=O$. Sąlyga pakankama.

Pavyzdys. Jeigu

$$f(x)=x^4-4,$$

tai $\sqrt{2}$ yra polinomo $f(x)$ šaknis, nes

$$f(x)=(x-\sqrt{2})\,(x+\sqrt{2})\,(x^2+2).$$

Tačiau 2 nėra to polinomo šaknis, nes pagal Hornerio schemą

	1	0	0	0	−4
2	1	2	4	8	12

gauname $f(2)=12\neq 0$.

Kai $f(x)=g(x)\,q(x)$, teiginys $f(l)=g(l)\,q(l)=O$ ekvivalentus teiginiui $(g(l)=0)\vee(q(l)=0)$. Taigi *polinomo šaknys sutampa su jo daugiklių šaknimis.*

Pagal Bezu teoremą

$$f(x)=(x-l)\,q(x),$$

kai l yra polinomo f šaknis. Iš pastarojo tvirtinimo išplaukia, kad polinomo $q(x)$ kiekviena šaknis yra polinomo $f(x)$ šaknis. Taigi tuo atveju, kai mus domina polinomo šaknų skaičius, gali kilti tam tikra painiava. Jeigu, pavyzdžiui,

$$f(x)=(x-l_1)\,q_1(x) \quad \text{ir} \quad q_1(x)=(x-l_2)\,q_2(x),$$

tai

$$f(x)=(x-l_1)\,(x-l_2)\,q_2(x).$$

Tuo atveju, kai $l_1\neq l_2$, polinomas $f(x)$ turi dvi šaknis l_1 ir l_2. Kai $l_1=l_2$, neaišku, kiek šaknų turi polinomas $f(x)$ – vieną ar dvi. Siekdami išvengti panašios painiavos, įvesime kartotinės šaknies sąvoką.

Sakoma, kad *polinomas* $f(x)$ *turi s-ojo kartotinumo šaknį* l $(s \geqslant 1)$, *jei* $f(x)$ *dalijasi iš* $(x-l)^s$, *bet nesidalija iš* $(x-l)^{s+1}$. Tuo atveju *skaičius* s *vadinamas šaknies* l *kartotinumu.* Kai $s=1$, šaknis l vadinama *paprastąja šaknimi.*

Pavyzdys. Jeigu

$$f(x)=x^5-\sqrt{2}\,x^4-4x+4\sqrt{2},$$

tai $\sqrt{2}$ yra antrojo kartotinumo šaknis, o $-\sqrt{2}$ – paprastoji šaknis, nes

$$f(x)=(x-\sqrt{2})^2\,(x+\sqrt{2})\,(x^2+2).$$

Kalbėdami apie polinomo virš integralumo srities $\check{\mathbf{Z}}$ šaknis, visada turime papildomai patikslinti, kur ieškosime šaknų, nes žiedo viršžiedis $\mathbf{Z}'$ apibrėžtas nevienareikšmiškai. Atskiru atveju mus domina, kiek šaknų polinomas $f(x)$ turi pačiame žiede $\check{\mathbf{Z}}$. Jeigu, pavyzdžiui, $\check{\mathbf{Z}}=\mathbf{Z}$, tai galime imti $Z'=\mathbf{Q}$, $Z'=\mathbf{R}$ arba $Z'=\mathbf{K}$. Tada kalbėtume apie polinomo su sveikaisiais koeficientais racionaliųjų, realiųjų arba kompleksinių šaknų skaičių. Atsakyti į klausimą, kiek šaknų nurodytame žiede turi polinomas, neįmanoma. Įrodysime, kad n-ojo laipsnio polinomo šaknų skaičius ne didesnis už n.

140 teorema. *Jeigu* $\check{\mathbf{Z}}$ *yra integralumo sritis, tai kiekvienas n-ojo* $(n \geqslant 1)$ *laipsnio polinomas virš* $\check{\mathbf{Z}}$ *integralumo srityje* $\check{\mathbf{Z}}$ *ir kiekviename jos plėtinyje, kuris irgi yra integralumo sritis, turi ne daugiau kaip n šaknų (įskaitant ir jų kartotinumą).*

Įrodymas. Tarkime, kad $\check{Z} \subset Z'$, o n-ojo laipsnio polinomas $f(x)$ žiede Z' turi šaknis $l_1, \ldots, l_m$, kurių kartotinumai atitinkamai yra $s_1, \ldots, s_m$. Remdamiesi Bezu teorema, gauname

$$f(x)=\left(\prod_{j=1}^{m}(x-l_j)^{s_j}\right) g_m(x), \quad q_m(x) \in Z'[x].$$

Kadangi polinomų virš integralumo srities sandaugos laipsnis lygus dauginamųjų laipsnių sumai, tai dešiniojoje lygybės pusėje esančios sandaugos laipsnis ne žemesnis už $s_1+\ldots+s_m$. Lygių polinomų laipsniai yra lygūs, todėl

$$s_1+\ldots+s_m \leqslant n.$$

Iš įrodytosios teoremos išplaukia įdomios ir svarbios išvados.

1 išvada. *Jeigu polinomo* $f(x)$ *virš integralumo srities* $\check{\mathbf{Z}}$ *laipsnis ne didesnis už m ir toje integralumo srityje tas polinomas turi n šaknų* $(n>m)$, *tai* $f(x)$ *yra nulinis polinomas.*

2 išvada. *n-ojo laipsnio polinomas virš lauko L vienareikšmiškai nustatomas jo reikšmėmis* $n+1$*-ame to lauko taške.*

Įrodymas. Skaičius n turi būti mažesnis už lauko L charakteristiką, kai ji nelygi nuliui, nes priešingu atveju lauke bus mažiau kaip $n+1$ skirtingas elementas.

Tarkime kad $\deg(f)=n$, $f(l_i)=b_i$, $i=1, 2, \ldots, n+1$, ir $l_1, \ldots, f_{n+1}$ yra lauko **L** skirtingi elementai.

Žymėkime

$$f(x)=\sum_{j=0}^{n} a_j x^j$$

ir koeficientus $a_0, a_1, \ldots, a_n$ laikykime nežinomais. Juos rasime iš $n+1$ tiesinių lygčių sistemos su $n+1$ kintamuoju:

$$\sum_{j=0}^{n} a_j l_i^j = b_i, \quad i=1, 2, \ldots, n+1.$$

Tos sistemos determinantas

$$\Delta=\begin{vmatrix} 1 & l_1 & l_1^2 & \ldots & l_2^n \\ 1 & l_2 & l_2^2 & \ldots & l_2^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & l_{n+1} & l_{n+1}^2 & \ldots & l_{n+1}^n \end{vmatrix} = \prod_{1\leqslant j<i\leqslant n+1} (l_i - l_j)$$

nelygus nuliui, kai $l_1, \ldots, l_{n+1}$ skirtingi. Taigi sistema, imant konkretų lauko **L** elementų rinkinį $b_1, b_2, \ldots, b_{n+1}$, turi vienintelį sprendinį.

Uždaviniai

19. Nustatykite, kurie iš šių skaičių yra polinomo šaknys, ir apskaičiuokite šaknų kartotinumą:

a) $2x^2-3x+1$, $l_1=0$, $l_2=1$, $l_3=\frac{1}{2}$;

b) x^3+x^2-5x+3, $l_1=3$, $l_2=-3$, $l_3=1$, $l_4=-1$;

c) $3x^5-4x^4+6x^3-2x^2-7x+4$, $l_1=2$, $l_2=1$, $l_3=-1$;

d) $4x^7-6x^5+5x^3-25x^2$, $l_1=\frac{1}{2}$, $l_2=0$, $l_3=-1$.

20. Nustatykite, kurios iš pateiktųjų l reikšmių yra polinomo šaknys. Nustatykite šaknų kartotinumą ir polinomą išreikškite pirmojo laipsnio polinomų sandauga:

a) $6x^4-x^3+4x^2-x-2$, $l\in\left\{-1, 1, -2, 2, -i, i, -\frac{1}{2}, \frac{1}{2}, -\frac{2}{3}, \frac{2}{3}\right\}$;

b) $4x^4-8x^3-3x^2+3x-2$, $l\in\left\{-2, 2, -1, 1, -\frac{1}{2}, \frac{1}{2}\right\}$;

c) $36x^5-120x^4+13x^3+73x^2-8x-12$,

$$l\in\left\{-3, 3, -1, 1, -\frac{1}{2}, \frac{1}{2}, -\frac{3}{2}, \frac{3}{2}\right\};$$

d) $25x^5-55x^4+19x^3+23x^2-8x+4$,

$$l\in\left\{-2, 2, -1, 1, -\frac{1}{2}, \frac{1}{2}, -\frac{2}{5}, \frac{2}{5}\right\}.$$

21. m-ojo laipsnio polinomas $g(x)$ turi skirtingas šaknis $l_1, \ldots, l_m$. Įrodykite, kad polinomas $f(x)$ dalijasi iš $g(x)$ tada ir tik tada, kai $l_1, \ldots, l_m$ yra ir polinomo $f(x)$ šaknys.

22. Remdamiesi 21 uždaviniu, įrodykite:

a) polinomas $f(x)=x^{3k}+x^{3l+1}+x^{3m+2}$, $k, l, m \in \mathbf{N}$, dalijasi iš polinomo $g(x)=x^2+x+1$;

b) polinomas $f(x)=x^{4k}+x^{4l+1}+x^{4m+2}+x^{4n+3}$, $k, l, m, m \in \mathbf{N}$, dalijasi iš polinomo $g(x)=x^3+x^2+x+1$.

69. Polinomų virš nulinės charakteristikos integralumo srities algebrinės ir funkcinės lygybių ekvivalentumas

65 paragrafe konstatavome, kad ne visada iš polinominių funkcijų lygybės išplaukia atitinkamų polinomų lygybė. Pateikiama teorema nurodo klasę integralumo sričių, virš kurių algebrinė ir funkcinė polinomų lygybės yra ekvivalenčios.

141 teorema. *Jeigu* $\check{Z}$ *yra nulinės charakteristikos integralumo sritis, tai polinomai* $f(x_1, \ldots, x_n) \in \check{Z}[x_1, \ldots, x_n]$ ir $g(x_1, \ldots, x_n) \in \check{Z}[x_1, \ldots, x_n]$ *yra lygūs tada ir tik tada, kai su kiekvienu rinkiniu*

$$(l_1, \ldots, l_n) \in \check{Z}^n$$

teisinga lygybė

$$f(l_1, \ldots, l_n) = g(l_1, \ldots, l_n).$$

Įrodymas. 1. Kadangi lygius polinomus atitinkančios polinominės funkcijos yra lygios (žr. § 61 ir 65), tai teoremos sąlyga būtina.

2. Sąlygos pakankamumą įrodysime matematinės indukcijos metodu.

Kai $n=1$, iš teoremos sąlygos su kiekvienu $l \in \check{Z}$ išplaukia $f(l)=g(l)$. Kadangi $\deg(f-g) \leqslant \max\{\deg(f), \deg(g)\}$, tai polinomas $f(x)-g(x)$ turi žiede $\check{Z}$ baigtinį skaičių šaknų (140 teorema). Kai $\operatorname{char} \check{Z}=0$, tada $\check{Z}$ – begalinė aibė ir

$$f(l)-g(l)=O$$

su be galo daug reikšmių l. Prieštaravimo nebus tik tuo atveju, kai $f(x)-g(x)=O(x)$. Taigi, kai $n=1$, sąlyga pakankama.

Tarkime, kad sąlyga pakankama ir kai $n=r$.

Kai $n=r+1$,

$$f(x_1, \ldots, x_{r+1}) = \sum_{j=0}^{s} f_j x_{r+1}^j, \quad g(x_1, \ldots, x_{r+1}) = \sum_{j=0}^{m} g_j x_{r+1}^j;$$

čia

$$g_j = g_j(x_1, \ldots, x_r) \quad \text{ir} \quad f_j = f_j(x_1, \ldots, x_r).$$

Kadangi su kiekvienu rinkiniu $l_1, \ldots, l_r, l_{r+1}$ iš $\check{Z}$

$$f(l_1, \ldots, l_r, l_{r+1}) = g(l_1, \ldots, l_r, l_{r+1}),$$

tai, imdami bet kokius $l_1, \ldots, l_r$, o l_{r+1} lygų O, gauname lygybę

$$f_0(l_1, \ldots, l_r) = g_0(l_1, \ldots, l_r)$$

su bet kuriais $l_1, \ldots, l_r$ iš $\check{Z}$. Taigi pagal prielaidą

$$f_0(x_1, \ldots, x_r) = g_0(x_1, \ldots, x_r). \tag{7.12}$$

Toliau nagrinėjame polinomus

$$\varphi_1(x_1, \ldots, x_{r+1}) = \sum_{j=1}^{s} f_j(x_1, \ldots, x_r)\, x_{r+1}^{j-1},$$

$$\psi_1(x_1, \ldots, x_{r+1}) = \sum_{j=1}^{m} g_j(x_1, \ldots, x_r)\, x_{r+1}^{j-1}.$$

Pagal teoremos sąlygą

$$\varphi_1(l_1, \ldots, l_r, l_{r+1}) = \psi_1(l_1, \ldots, l_r, l_{r+1})$$

su kiekvienu rinkiniu $l_1, \ldots, l_r, l_{r+1}$ iš $\check{Z}$. Imdami bet kokius $l_1, \ldots, l_r$ iš $\check{Z}$, o l_{r+1} lygų O, gauname lygybes

$$f_1(l_1, \ldots, l_r) = g_1(l_1, \ldots, l_r),$$

iš kurių išplaukia

$$f_1(x_1, \ldots, x_r) = g_1(x_1, \ldots, x_r). \tag{7.13}$$

Tą procesą tęsdami toliau, analogiškai sudarome polinomus

$$\varphi_k(x_1, \ldots, x_{r+1}) = \sum_{j=k}^{s} f_j(x_1, \ldots, x_r)\, x_{r+1}^{j-k},$$

$$\psi_k(x_1, \ldots, x_{r+1}) = \sum_{j=k}^{m} g_j(x_1, \ldots, x_r)\, x_{r+1}^{j-k}$$

($k=2, \ldots, \max\{s, m\}$). Iš teoremos sąlygos ir indukcijos prielaidos gauname

$$f_k(x_1, \ldots, x_r) = g_k(x_1, \ldots, x_r) \quad (k=2, \ldots, \max\{s, m\}). \tag{7.14}$$

(7.12)–(7.14) lygybės reiškia, kad $f_j(x_1, \ldots, x_r) = g_j(x_1, \ldots, x_r)$ su visais $j=0, 1, 2, \ldots$

Taigi tarę, kad sąlyga pakankama, kai $n=r$, gauname, jog ji yra pakankama ir kai $n=r+1$. Todėl sąlyga pakankama su kiekvienu natūriniu n.

§70. Algebriniai elementai

59 paragrafe apibrėžėme transcendentinio integralumo srities $\check{Z}$ atžvilgiu elemento sąvoką. Pasinaudoję vieno kintamojo polinomo šaknies apibrėžimu, galime konstatuoti: *jeigu elementas* β *yra transcendentinis integralumo srities* $\check{Z}$ *atžvilgiu, tai nėra nenulinio polinomo virš* $\check{Z}$, *kurio šaknis būtų* β.

Šis teiginys išplaukia iš tokių samprotavimų. Sakykime,

$$f(x)=\sum_{j=0}^{n} a_j x^j, \quad n\geqslant 0,$$

yra toks polinomas, kad $f(\beta)=O$. Kadangi β – transcendentinis $\check{\mathbf{Z}}$ atžvilgiu, tai iš lygybės

$$f(\beta)=\sum_{j=0}^{n} a_t \beta^j = O$$

išplaukia $a_j=O$, $j=0, 1, \ldots, n$. Taigi $f(x)=O(x)$.

Elementas α, kuris yra kokio nors nenulinio laipsnio polinomo virš integralumo srities $\check{\mathbf{Z}}$ šaknis, vadinamas algebriniu $\check{\mathbf{Z}}$ atžvilgiu.

Pavyzdžiui, *kiekvienas racionalusis skaičius yra algebrinis sveikųjų skaičių žiedo atžvilgiu.* Tuo įsitikinsime, paėmę racionalųjį skaičių

$$\frac{a}{b} \quad (b\neq O,\ a,\ b\in\mathbf{Z})$$

ir polinomą $f(x)=bx-a$. Gausime

$$f\left(\frac{a}{b}\right)=b\cdot\frac{a}{b}-a=O.$$

Skaičius $i=(0, 1)$ yra algebrinis sveikųjų skaičių žiedo $\mathbf{Z}$ atžvilgiu, nes i yra polinomo $f(x)=x^2+1$ šaknis.

Skaičiai, algebriniai sveikųjų skaičių žiedo atžvilgiu, vadinami algebriniais skaičiais; skaičiai, transcendentiniai sveikųjų skaičių žiedo atžvilgiu, vadinami transcendentiniais skaičiais.

Jeigu integralumo sritis yra laukas, $\check{\mathbf{Z}}=\mathbf{L}$, tai kiekvienas elementas $\alpha\in L$ yra algebrinis $\mathbf{L}$ atžvilgiu. Tai išplaukia iš šio teiginio: jeigu

$$f(x)=x-\alpha, \quad \text{tai} \quad f(\alpha)=\alpha-\alpha=O.$$

Yra laukų, virš kurių ne visi polinomai turi šaknų tame lauke. Pavyzdžiui, toks yra racionaliųjų skaičių laukas $\mathbf{Q}$, nes polinomas $f(x)=x^2-2$ su sveikaisiais koeficientais neturi racionaliųjų šaknų. Realiųjų skaičių laukui $\mathbf{R}$ irgi būdinga tokia savybė, nes polinomas $f(x)=x^2+1$ neturi realiųjų šaknų.

Laukas **L** *vadinamas algebriškai uždaru, jei kiekvienas nenulinio laipsnio polinomas virš* **L** *turi šaknį tame lauke. Priešingu atveju laukas vadinamas algebriškai neuždaru.*

Taigi *racionaliųjų skaičių laukas* **Q** *ir realiųjų skaičių laukas* **R** *nėra algebriškai uždari.*

Ne visi polinomai virš integralumo srities $\check{Z}$, kuri nėra laukas, turi šaknį toje srityje. Tuo įsitikiname paėmę elementą $a \in \check{Z}$, $a \neq O$, kuris neturi atvirkštinio, ir įrodę, jog polinomo $ax+b$ šaknis $-b/a$ nepriklauso $\check{Z}$. Polinomo $ax+b$ šaknis $-b/a$ priklauso tos integralumo srities santykių laukui. Taigi *jokia integralumo sritis, kuri nėra laukas, negali būti algebriškai uždara.*

Jeigu elementas α algebrinis $\check{Z}$ atžvilgiu, tai yra toks polinomas $f(x) \in \check{Z}[x]$, $\deg(f) \geqslant 1$, kad $f(\alpha)=O$. Jeigu polinomas $f(x)$ turi kokį nors tiesioginį daliklį $g(x)$, tai $f(x)=g(x)\,q(x)$ ir $q(x)$ irgi yra polinomo $f(x)$ tiesioginis daliklis. Be to, $f(\alpha)=g(\alpha)q(\alpha)=O$, todėl $(g(\alpha)=O) \vee (q(\alpha)=O)$. Kadangi polinomo neasocijuotų tiesioginių daliklių aibė baigtinė, tai yra toks žemiausio laipsnio polinomas $p(x) \in \check{Z}[x]$, kad $p(\alpha)=O$.

Žemiausio laipsnio polinomo $p(x) \in \check{Z}[x]$, *kurio šaknis yra elementas* α, *laipsnis vadinamas algebrinio elemento* α *laipsniu. Visos to polinomo šaknys vadinamos elementui* α *jungtiniais elementais.*

Pavyzdžiai. 1. Menamasis vienetas i yra antrojo laipsnio algebrinis skaičius (virš **Z**), nes žemiausio laipsnio polinomas, kurio šaknis i, yra x^2+1. Kita to polinomo šaknis yra $-i$. Taigi i ir $-i$ – jungtiniai algebriniai antrojo laipsnio skaičiai.

2. Žemiausio laipsnio polinomas, kurio šaknis $a+ib$, $b \neq 0$, $a, b \in \mathbf{R}$, yra $x^2-2ax+(a^2+b^2)$. Kita to polinomo šaknis yra $a-ib$. Taigi $a+ib$ ir $a-ib$ yra jungtiniai algebriniai antrojo laipsnio skaičiai virš **R**.

3. Žemiausio laipsnio polinomas, kurio šaknis $1+\sqrt{2}$, yra x^2-2x-1. Kita to polinomo šaknis yra $1-\sqrt{2}$. Taigi $1-\sqrt{2}$ ir $1+\sqrt{2}$ – jungtiniai algebriniai antrojo laipsnio skaičiai.

Uždaviniai

23. Nustatykite, ar šie skaičiai yra algebriniai racionaliųjų skaičių lauko atžvilgiu, raskite jų laipsnius:

a) $\alpha=\sqrt{2}$; b) $\alpha=\sqrt{2}+3$; c) $\alpha=\sqrt{5}$;

d) $\alpha=\sqrt{3}-\sqrt{5}$; e) $\alpha=\sqrt[4]{3}-1$; f) $\alpha=\dfrac{\sqrt[3]{2}}{\sqrt{3}}$.

24. Įrodykite, kad kiekvienas skaičius, kuris yra algebrinis racionaliųjų skaičių lauko atžvilgiu, yra algebrinis ir sveikųjų skaičių žiedo atžvilgiu.

25. Įrodykite, kad kiekvienas menamasis skaičius $a+ib$ $(b \neq 0)$ yra algebrinis realiųjų skaičių lauko atžvilgiu.

Vieno kintamojo polinomų virš lauko žiedas

§71. Dalybos su liekana teorema

Šiame skyriuje nagrinėsime vieno kintamojo polinomus virš lauko **L**, t. y. žiedą **L** $[x]$. Kadangi kiekvienas laukas yra integralumo sritis, tai žiedui **L** $[x]$ būdingos visos savybės, nagrinėtos VII skyriuje. Be to, žiedas **L** $[x]$ turi dar ir kitų savybių, kurių neturi polinomų virš integralumo srities žiedas.

Kiekvienas polinomas virš lauko **L** *dalijasi iš kiekvieno nelygaus nuliui lauko* **L** *elemento* c.

Kai $c \neq O$, egzistuoja $c^{-1} \in L$, $cc^{-1} = e$ ir kiekvieną polinomą $f(x) \in L[x]$ galima užrašyti šitaip:

$$f(x) = ef(x) = c\left(c^{-1}f(x)\right) = cg(x),\ g(x) = c^{-1}f(x).$$

Iš to išplaukia, kad *polinomai* $f(x)$ *ir* $g(x)$ *iš* $L[x]$ *yra asocijuoti, kai* $f(x) = cg(x)$ *ir* $c \neq O$.

Polinomų virš lauko **L** žiede yra dalybos su liekana teoremos analogas.

142 (dalybos su liekana) teorema. *Kad ir kokie būtų du polinomai* $f(x)$ *ir* $g(x) \neq O(x)$ *iš* $L[x]$, *egzistuoja vieninteliai tokie polinomai* $q(x)$ *ir* $r(x)$ *iš* $L[x]$, *su kuriais*

$$f(x) = g(x)q(x) + r(x).$$

Polinomas $r(x)$ *yra arba nulinis, arba* $\deg(r) < \deg(g)$.

Polinomas $q(x)$ vadinamas *nepilnuoju santykiu*, o $r(x)$ — *liekana, gautais dalijant polinomą* $f(x)$ *iš polinomo* $g(x)$.

Įrodymas. Kai $\deg(g) = 0$, t. y. $g(x) = c \neq O$,

$$f(x) = c\left(c^{-1}f(x)\right) + O.$$

Taigi šiuo atveju $q(x) = c^{-1}f(x)$, $r(x) = O(x)$. Lieka išnagrinėti atvejį, kai $\deg(g) \geqslant 1$.

Tarkime, kad

$$f(x) = \sum_{j=0}^{n} a_j x^j,\ g(x) = \sum_{j=0}^{m} b_j x^j,\quad b_m \neq O,\ m \geqslant 1.$$

Kai $n < m$, teoremos tvirtinimas išplaukia iš lygybės

$$f(x) = g(x) \cdot o(x) + f(x).$$

Taigi tuo atveju $q(x) = o(x)$, $r(x) = f(x)$.

Kai $n \geqslant m$, sudarome polinomą g_1:

$$g_1(x) = a_n b_m^{-1} x^{n-m} g(x).$$

To polinomo vyriausiasis narys yra $a_n x^n$, todėl

$$f(x) - g_1(x) = f_1(x)$$

yra polinomas iš $L[x]$ ir jo laipsnis n_1 mažesnis už n. Jeigu $n_1 \geqslant m$, sudarome polinomą g_2:

$$g_2(x) = a_{n_1}^{(1)} b_m^{-1} x^{n_1-m} g(x);$$

čia $a_{n_1}^{(1)}$ – polinomo $f_1(x)$ vyriausiasis koeficientas. Polinomo $g_2(x)$ vyriausiasis narys yra $a_{n_1}^{(1)} x^{n_1}$, t. y. sutampa su polinomo $f_1(x)$ vyriausiuoju nariu. Taigi

$$f_1(x) - g_2(x) = f_2(x)$$

yra polinomas iš $L[x]$, ir jo laipsnis n_2 mažesnis už n_1. Jeigu $n_2 \geqslant m$, tai procesą tęsiame. Po $s+1$ žingsnio gaunam̃e lygybes

$$\begin{aligned} f(x) &= g_1(x) + f_1(x), \\ f_1(x) &= g_2(x) + f_2(x), \\ &\cdots\cdots\cdots\cdots \\ f_{s-1}(x) &= g_s(x) + f_s(x), \\ f_s(x) &= g_{s+1}(x) + f_{s+1}(x), \end{aligned} \tag{8.1}$$

kuriose visi polinomai yra iš $L[x]$. Be to, polinomų $f_j(x)$ laipsniai n_j ($j = 1, 2, \ldots, s$) tenkina nelygybes:

$$m \leqslant n_s < n_{s-1} < \ldots < n_2 < n_1 < n.$$

Taigi po baigtinio žingsnių skaičiaus $s+1$, $s \leqslant n-m$, gauname polinomą $f_{s+1}(x)$, kurio laipsnis mažesnis už m.

Pažymėję polinomų $f_j(x)$ vyriausiuosius koeficientus $a_{n_j}^{(j)}$ ir pažymėję

$$d_j(x) = a_{n_j}^{(j)} b_m^{-1} x^{n_j-m},$$

užrašome lygybes

$$g_j(x) = d_j(x)\, g(x) \quad (j = 1, \ldots, s+1). \tag{8.2}$$

Iš (8.1) lygybių, remdamiesi (8.2) lygybėmis ir distributyvumo savybe, gauname

$$f(x) = \sum_{j=1}^{s+1} g_j(x) + f_{s+1}(x) = g(x) \sum_{j=1}^{s+1} d_j(x) + f_{s+1}(x).$$

Pažymėję

$$q(x) = \sum_{j=1}^{s+1} d_j(x) \quad \text{ir} \quad r(x) = f_{s+1}(x),$$

gauname $f(x) = g(x)\, q(x) + r(x)$, $q(x) \in L[x]$, $r(x) \in L[x]$, ir, be to, $\deg(r) < \deg(g)$.

Įsitikinsime, kad $q(x)$ ir $r(x)$ randami vienareikšmiškai. Tuo tikslu tariame, jog

$$f(x)=g(x)\,q(x)+r(x),\ f(x)=g(x)\,q_1(x)+r_1(x)$$

ir $r(x)=O(x)$, arba $\deg(r)<\deg(g)$ ir $r_1(x)=O(x)$, arba $\deg(r_1)<\deg(g)$.

Atlikę akivaizdžius pertvarkius, gausime lygybę

$$g(x)\big(q(x)-q_1(x)\big)=r_1(x)-r(x).$$

Jeigu $q(x)-q_1(x)\neq O(x)$, tai $r_1(x)-r(x)=O(x)$ arba $\deg(r_1-r)<\deg(g)$. Kiekvienu atveju prieštaravimas reiškia, kad $q(x)-q_1(x)=O(x)$. Taigi $q(x)=q_1(x)$. Tuomet

$$g(x)\big(q(x)+q_1(x)\big)=O(x)\quad\text{ir}\quad r_1(x)+r(x)=O(x).$$

Tarę, kad $f(x)$ ir $g(x)$ yra polinomai virš integralumo srities $\check{Z}$ ir b_m, polinomo $g(x)$ vyriausiasis koeficientas, yra vieneto daliklis, t. y. b_m^{-1} irgi tos srities elementas, gausime polinomus

$$d_j(x)=a_{n_j}^{(j)}b_m^{-1}x^{n_j-m}\in\check{Z}[x].$$

Taigi

$$q(x)=\sum_{j=1}^{s+1}d_j(x)\in\check{Z}[x],\ r(x)=f(x)-g(x)\,q(x)\in\check{Z}[x].$$

Todėl teoremos apie dalybą su liekana dalinis atvejis yra teisingas ir polinomų virš integralumo srities žiede.

1 išvada. *Jeigu $f(x)$ yra bet kuris polinomas virš integralumo srities $\check{Z}$, $g(x)$ irgi polinomas virš tos pačios srities ir jo vyriausiasis koeficientas yra žiedo $\check{Z}$ vieneto daliklis, tai egzistuoja vieninteliai polinomai virš $\check{Z}$ $q(x)$ ir $r(x)$, su kuriais*

$$f(x)=g(x)\,q(x)+r(x)$$

ir $r(x)=O(x)$ arba $\deg(r)<\deg(g)$.

Kai $\check{Z}$ yra sveikųjų skaičių žiedas, ta išvada reiškia, kad *polinomą su sveikaisiais koeficientais dalijant iš polinomo su sveikaisiais koeficientais, kurio vyriausiasis koeficientas lygus 1 arba -1, gaunami nepilnasis santykis ir liekana yra polinomai su sveikaisiais koeficientais.*

Teoremos įrodymas ne tik patvirtina, kad polinomai $q(x)$ ir $r(x)$ egzistuoja, bet yra ir metodas jiems rasti. Tas metodas vadinamas dalybos su liekana algoritmu. Jis primena skaičių dalybą kampu dešimtainėje skaičiavimo sistemoje.

Pavyzdys. Duoti polinomai

$$f(x)=4x^5-6x^2+3x-15,\ g(x)=x^3+2x^2-6x+4.$$

Rasime tokius polinomus $q(x)$ ir $r(x)$, kad būtų

$$f(x)=g(x)\,q(x)+r(x).$$

Sprendimas.

$$\begin{array}{l|l} 4x^5 - 6x^2+3x-15 & x^3+2x^2-6x+4 \\ \hline 4x^5+8x^4-24x^3+16x^2 & 4x^2-8x+40 \\ \hline -8x^4+24x^3-22x^2+3x-15 & \\ -8x^4-16x^3+48x^2-32x & \\ \hline 40x^3-70x^2+35x-15 & \\ 40x^3+80x^2-240x+160 & \\ \hline -150x^2-275x-175 & \end{array}$$

Taigi

$$4x^5-6x^2+3x-15=(x^3+2x^2-6x+4)(4x^2-8x+40)+(-150x^2+275x-175),$$

t. y.

$$q(x)=4x^2-8x+40,\ r(x)=-150x^2+275x-175.$$

Iš dalybos su liekana teoremos išplaukia dar dvi išvados, kurios išsamiau paaiškina polinomų virš lauko **L** žiedo **L** [x] struktūrą.

2 išvada. *Polinomų virš lauko* **L** *žiedas* **L** [x] *yra Euklido žiedas.*

Įrodymas. Kiekvieno $f(x)\in L[x]$ $\deg(f)$ yra sveikasis neneigiamas skaičius. Vadinasi, aibėje $L[x]\setminus\{O(x)\}$ galime apibrėžti funkciją, įgyjančią sveikąsias neneigiamas reikšmes ir turinčią šias savybes:

1. Jeigu $f(x)\,g(x)\neq O(x)$, tai $\deg(fg)\geqslant\deg(f)$ — tai išplaukia iš lygybės $\deg(fg)=\deg(f)+\deg(g)$;

2. Kiekvienai polinomų iš $L[x]$ porai $f(x)$ ir $g(x)\neq O(x)$ egzistuoja tokie polinomai $q(x)$ ir $r(x)$ iš $L[x]$, su kuriais

$$f(x)=g(x)\,q(x)+r(x)$$

ir, be to, arba $r(x)=O(x)$, arba $\deg(r)<\deg(g)$ (dalybos su liekana teorema).

Remdamiesi Euklido žiedo apibrėžimu (žr. § 57), tvirtiname, kad išvada yra teisinga.

3 išvada. *Polinomų virš lauko* **L** *žiedas* **L** [x] *yra vyriausiųjų idealų žiedas.*

Įrodymas išplaukia iš 2 išvados ir to fakto, kad kiekvienas Euklido žiedas yra vyriausiųjų idealų žiedas (žr. 119 teoremą).

Taigi kiekvienas žiedo **L** [x] idealas yra

$$\{g(x)f(x)\,|\,f(x)\in L[x]\},$$

t. y. polinomo $g(x)$ kartotinių aibė.

Uždaviniai

1. Polinomą $f(x)$ padalykite su liekana iš polinomo $g(x)$:

a) $f(x)=3x^5-7x^4+3x^3-5x^2+13x-28$, $g(x)=x^3-2x+1$;

b) $f(x)=16x^7-13x^5+11x^2-60$, $g(x)=3x^7-4x^6-8x$;

c) $f(x)=14x^6-7x^5-3x^3+13$, $g(x)=\frac{1}{3}$;

d) $f(x)=28x^3-14x^2+9x-17$, $g(x)=7x^9+8x^6+3x^3-58x+120$;

e) $f(x)=x^3+x^2-5x+3$, $g(x)=x^2-2x+1$.

2. Remdamiesi dalybos su liekana teorema, nustatykite, ar polinomas $f(x)$ dalijasi iš polinomo $g(x)$:

a) $f(x)=x^7+2x^6+3x^5-x^3-2x-3$, $g(x)=x^4+x^3+x^2+x+1$;
b) $f(x)=5x^7+6x^6-2x^4+5x^3+6x^2-4$, $g(x)=5x^3+6x^2-2$;
c) $f(x)=4x^6+5x^5-3x^4+4x^3-2x^2+1$, $g(x)=2x^2-5x+3$.

3. Raskite tokias a ir b reikšmes, kad $f(x)$ dalytųsi iš $g(x)$:

a) $f(x)=x^3+ax+2$, $g(x)=x+1$;
b) $f(x)=x^4+ax+b$, $g(x)=x^2+x+1$;
c) $f(x)=x^4+ax^3+b$, $g(x)=x^2-1$;

4. Raskite polinomų žiedo $\mathbf{Z}[x]$ gretimas klases pagal idealą $(g(x))$, kurioms priklauso polinomai $f(x)=3x^2+6x-1$, $\varphi(x)=3x^3-6x^2+4x+4$, tų klasių sumą ir sandaugą, kai:

a) $g(x)=x-1$; b) $g(x)=x+1$; c) $g(x)=x+2$;
d) $g(x)=x^2-2$; e) $g(x)=x^2+3$.

§72. Polinomų bendrieji dalikliai. Polinomų didžiausias bendrasis daliklis

Jeigu polinomai $f_1(x), \ldots, f_m(x)$, $m\geqslant 2$, *iš* $L[x]$ *dalijasi iš nenulinio polinomo* $g(x)\in L[x]$, *tai polinomas* $g(x)$ *vadinamas polinomų* $f_1(x), \ldots, f_m(x)$ *bendruoju dalikliu.*

Polinomų virš lauko žiede $\mathbf{L}[x]$ bet kurie polinomai $f_1(x), \ldots, f_m(x)$ turi bendrąjį daliklį – nulinio laipsnio polinomą $c\neq O$.

Nulinio laipsnio bendrieji dalikliai vadinami *trivialiaisiais*, o nenulinio laipsnio bendrieji dalikliai – *netrivialiaisiais*, arba *tiesioginiais*, *bendraisiais dalikliais.*

Polinomai $f_1(x), \ldots, f_m(x)$, $m\geqslant 2$, *virš* $\mathbf{L}$, *neturintys bendrųjų daliklių, išskyrus trivialiuosius, vadinami tarpusavyje pirminiais polinomais.*

Pavyzdys. Polinomai

$$f_1(x)=3x^3+6x+5,\ f_2(x)=x^2-5x+6$$

neturi bendrųjų nenulinio laipsnio daliklių, taigi jie yra tarpusavyje pirminiai.

Polinomai

$$g_1(x)=3x^3+3x^2-x-5,\ g_2(x)=(5x^3-3x^2+5)(5x-5)$$

turi netrivialų bendrąjį daliklį $x-1$, taigi jie nėra tarpusavyje pirminiai.

Aptarsime polinomų bendrųjų daliklių savybes.

1. *Jeigu polinomų* $f_1(x), \ldots, f_m(x)$ *iš* $L[x]$ $(m\geqslant 2)$ *bendrasis daliklis yra* $g(x)$, *tai su kiekvienu rinkiniu* $1\leqslant i_1<i_2<\ldots<i_k\leqslant m$ *polinomų* $f_{i_1}(x), \ldots, f_{i_k}(x)$ *bendrasis daliklis irgi yra* $g(x)$.

Ta savybė išplaukia iš apibrėžimo.

2. *Jeigu kurie nors du polinomai* $f_i(x)$ *ir* $f_j(x)$ *iš* $f_1(x), \ldots, f_m(x) \in L[x]$ $(m \geqslant 2)$ *neturi netrivialių bendrųjų daliklių, tai ir visi polinomai* $f_1(x), \ldots, f_m(x)$ *neturi netrivialių bendrųjų daliklių.*

Tarkime, kad $g(x) \mid f_k(x)$, $k=1, 2, \ldots, m$. Tuomet $g(x) \mid f_i(x)$ ir $g(x) \mid f_j(x)$, bet tai prieštarauja sąlygai.

3. *Jeigu* $f(x)=g(x)\,q(x)+r(x)$, *tai polinomų* $f(x)$ *ir* $g(x)$ *bendrųjų daliklių aibė sutampa su polinomų* $g(x)$ *ir* $r(x)$ *bendrųjų daliklių aibe.*

Įrodymas. Tarkime, kad $d(x) \mid f(x)$ ir $d(x) \mid g(x)$. Kadangi $r(x)=f(x)-g(x)\,q(x)$, tai pagal 7 ir 8 dalumo savybes $d(x) \mid r(x)$.

Jeigu $\delta(x) \mid g(x)$ ir $\delta(x) \mid r(x)$, tai pagal tas pačias dalumo savybes $\delta(x) \mid f(x)$.

143 teorema. *Du nelygūs nuliui polinomai* $f(x)$, $g(x) \in L[x]$ *turi netrivialų bendrąjį daliklį tada ir tik tada, kai egzistuoja tokie nenuliniai polinomai* $f_1(x)$, $g_1(x) \in L[x]$, $\deg(f_1) < \deg(f)$, $\deg(g_1) < \deg(g)$, *kad*

$$f(x)\,g_1(x)+g(x)\,f_1(x)=O(x).$$

Įrodymas. Būtinumas. Jeigu $d(x) \mid f(x)$ ir $d(x) \mid g(x)$, tai $f(x)=d(x)\,f_1(x)$, $g(x)=d(x)\,g_1(x)$, $\deg(f_1) < \deg(f)$ ir $\deg(g_1) < \deg(g)$. Todėl

$$f(x)\,g_1(x)+g(x)\,(-f_1(x))=d(x)\,(g_1(x)\,f_1(x)-g_1(x)\,f_1(x))=O(x).$$

Pakankamumas. Tarkime, kad

$$f(x)\,g_1(x)+g(x)\,f_1(x)=O(x)$$

ir $\deg(f_1) < \deg(f)$, $\deg(g_1) < \deg(g)$.

Kadangi $f(x) \mid f(x)\,g_1(x)$ ir $f(x) \mid O(x)$, tai $f(x) \mid g(x)\,f_1(x)$. Tačiau $(x)+f_1(x)$, todėl $g(x)$ ir $f(x)$ turi nenulinio laipsnio bendrąjį daliklį.

Polinomų $f_1(x), \ldots, f_m(x) \in L[x]$ $(m \geqslant 2)$, *iš kurių bent vienas nelygus nuliui, didžiausiu bendruoju daliklių vadinamas toks jų bendrasis daliklis, kuris dalijasi iš kiekvieno tų polinomų bendrojo daliklio. Didžiausias bendrasis daliklis* (d. b. d.) *žymimas* $\mathrm{D}(f_1(x), \ldots, f_m(x))$.

Polinomų didžiausias bendrasis daliklis nustatomas pastovaus daugiklio $c \neq O$ $(c \in L)$ *tikslumu,* nes *jeigu* $\delta(x)=\mathrm{D}(f_1, \ldots, f_m)$, *tai su kiekvienu lauko* **L** *elementu* c $(c \neq O)$ *polinomas* $c\delta(x)$ *taip pat yra polinomų* $f_1, \ldots, f_m$ *didžiausias bendrasis daliklis.*

Kadangi polinomų žiedas **L**$[x]$ yra Euklido žiedas, tai iš 142 teoremos 3 išvados ir 113 teoremos išplaukia, kad *bet kurių polinomų* $f_1(x), \ldots, f_m(x) \in L[x]$ $(m \geqslant 2)$, tarp kurių yra bent vienas nenulinis polinomas, *didžiausias bendrasis daliklis egzistuoja ir gali būti išreikštas šitaip*:

$$\mathrm{D}(f_1(x), \ldots, f_m(x))=\sum_{j=1}^{m} f_j(x)\,g_j(x);$$

čia $g_1(x), \ldots, g_m(x)$ – polinomai iš $L[x]$. *Pastaroji išraiška vadinama polinomų didžiausio bendrojo daliklio tiesine išraiška.*

Kadangi $\mathbf{L}[x]$ yra Euklido žiedas, tai dviejų polinomų $f(x)$ ir $g(x) \neq O(x)$ iš $L[x]$ didžiausią bendrąjį daliklį galima rasti remiantis 121 teorema. Polinomams ji formuluojama šitaip.

Dviejų polinomų $f(x)$ ir $g(x) \neq O(x)$ virš lauko didžiausias bendrasis daliklis lygus (asocijuotas) tų polinomų Euklido algoritmo paskutinei nelygiai nuliui liekanai.

Prisiminę Euklido algoritmą Euklido žiedo elementams, galime jį suformuluoti ir polinomams.

Polinomų $f(x)$ ir $g(x) \neq O(x)$ iš $L[x]$ *Euklido algoritmu* vadiname procesą, kuriuo randame tokius polinomus $q_0(x)$, $q_1(x)$, ..., $q_m(x)$ ir $r_1(x)$, $r_2(x)$, ..., $r_m(x)$, $\deg(g) > \deg(r_1) > \ldots > \deg(r_m)$, virš $\mathbf{L}$, su kuriais teisingos lygybės

$$\begin{aligned}
f(x) &= g(x)\,q_0(x) + r_1(x),\\
g(x) &= r_1(x)\,q_1(x) + r_2(x),\\
r_1(x) &= r_2(x)\,q_2(x) + r_3(x),\\
&\cdots\cdots\cdots\cdots\cdots\\
r_{m-2}(x) &= r_{m-1}(x)\,q_{m-1}(x) + r_m(x),\\
r_{m-1}(x) &= r_m(x)\,q_m(x).
\end{aligned}$$

Tas procesas yra baigtinis. Polinomus $q_j(x)$ ir $r_{j+1}(x)$ galima rasti remiantis dalybos su liekana teorema.

Atkreipsime dėmesį, kad $r_1(x) = O(x)$, kai $g(x) \mid f(x)$, ir tada $m = 0$, t. y. Euklido algoritme nėra nelygios nuliui liekanos. Tuo atveju $\mathrm{D}(f, g) = \mathrm{D}(gq_0, g) = g$.

Pastaba. Kadangi polinomų didžiausias bendrasis daliklis randamas pastovaus daugiklio tikslumu, tai dviejų polinomų Euklido algoritmą galima modifikuoti įvedant pastovius nenulinius daugiklius. Taip padarius, supaprastėja skaičiavimai.

Dviejų polinomų $f(x)$ ir $g(x) \neq O(x)$ *didžiausio bendrojo daliklio tiesinę išraišką*

$$\mathrm{D}\big(f(x),\ g(x)\big) = f(x)\,u(x) + g(x)\,v(x),$$

t. y. polinomus $u(x)$ ir $v(x)$, galime rasti taikydami Euklido algoritmą. Skaičiuojama taip pat, kaip ir ieškant dviejų sveikųjų skaičių didžiausio bendrojo daliklio tiesinės išraiškos.

Pavyzdys. Raskime polinomų $f(x) = 3x^5 + 9x^4 + x^3 + 6x + 1$ ir $g(x) = x^4 + x^3 - x^2 + x - 2$ didžiausią bendrąjį daliklį ir jo tiesinę išraišką.

1. Sudarome Euklido algoritmą naudodamiesi daugikliais:

$$\begin{array}{l|l}
3x^5 + 9x^4 + x^3 + 6x + 1 & x^4 + x^3 - x^2 + x - 2 \\
\underline{3x^5 + 3x^4 - 3x^3 + 3x^2 - 6x} & \overline{3x - 3 = q_0(x)} \\
-3x^4 + 12x^3 - 2x^2 + 12x + 1 & \\
\underline{-3x^4 - 3x^3 + 3x^2 - 3x + 6} & \\
15x^3 - 5x^2 + 15x - 5 = 5(3x^3 - x^2 + 3x - 1) = 5r_1(x). &
\end{array}$$

$$
\begin{array}{l|l}
9x^4+9x^3-9x^2+9x-18 & 3x^3-x^2+3x-1 \\
\underline{9x^4-3x^3+9x^2-3x} & \overline{3x+4=q_1(x)} \\
12x^3-18x^2+12x-18 & \\
\underline{12x^3-4x^2+12x-4} & \\
-14x^2-14=-14(x^2+1)=-14r_2(x). &
\end{array}
$$

$$
\begin{array}{l|l}
3x^3-x^2+3x-1 & x^2+1 \\
\underline{3x^3\quad +3x} & \overline{3x-1=q_2(x)} \\
-x^2-1 & \\
\underline{-x^2-1} & \\
0. &
\end{array}
$$

Pasinaudoję daugikliais, gauname šitokias modifikuoto Euklido algoritmo lygybes:

1) $f(x)=g(x)\,q_0(x)+5r_1(x)$,
2) $9g(x)=r_1(x)\,q_1(x)-14r_2(x)$,
3) $r_1(x)=r_2(x)\,q_2(x)$;

čia $r_2(x)=x^2+1$, $q_0(x)=3x-3$, $q_1(x)=3x+4$, $D(f(x), g(x))=x^2+1$, nes paskutinė nelygi nuliui liekana yra $r_2(x)$.

2. Rasime $D(f, g)$ tiesinę išraišką. Iš 2 lygybės gauname

$$r_2(x)=\frac{1}{14}\left(r_1(x)\,q_1(x)-9g(x)\right).$$

Iš 1 lygybės randame

$$r_1(x)=\frac{1}{5}\left(f(x)-g(x)\,q_0(x)\right),$$

todėl

$$r_2(x)=\frac{1}{14}\left(\frac{1}{5}f(x)\,q_1(x)-\frac{1}{5}g(x)\,q_0(x)\,q_1(x)-9g(x)\right)=$$

$$=f(x)\left(\frac{1}{70}q_1(x)\right)+g(x)\left(-\frac{1}{14}\left(\frac{1}{5}q_0(x)\,q_1(x)+9\right)\right).$$

Taigi

$$u(x)=\frac{1}{70}(3x+4),$$

$$v(x)=-\frac{1}{70}\left((3x-3)(3x+4)+45\right)=-\frac{3}{70}(3x^2+x+11).$$

$D(f, g)$ tiesinė išraiška yra

$$D(f, g)=x^2+1=f(x)\left(\frac{1}{70}(3x+4)\right)+g(x)\left(-\frac{3}{70}(3x^2+x+11)\right).$$

Tarpusavyje pirminių polinomų savybės.

Polinomai $f(x)$, $g(x)\in L[x]$ *vadinami tarpusavyje pirminiais, kai* $D(f, g)=e$.

1. *Polinomai $f(x)$ ir $g(x)$ virš* **L** *yra tarpusavyje pirminiai tada ir tik tada, kai egzistuoja virš lauko* **L** *tokie polinomai $u(x)$ ir $v(x)$, su kuriais teisinga lygybė*

$$f(x)\,u(x)+g(x)\,v(x)=e.$$

Įrodymas. Pakankamumas. Jeigu

$$f(x)\,u(x)+g(x)\,v(x)=e$$

ir $d(x)\mid f(x)$, $d(x)\mid g(x)$, tai $d(x)\mid e$. Taigi $d(x)=e\in L$.

Būtinumas išplaukia iš apibrėžimo ir polinomų d. b. d. tiesinės išraiškos.

2. *Jeigu $g(x)\mid f(x)\,h(x)$, o $f(x)$ ir $g(x)$ – tarpusavyje pirminiai polinomai, tai $g(x)\mid h(x)$.*

Įrodymas. Pagal 1 savybę

$$f(x)\,u(x)+g(x)\,v(x)=e.$$

Šią lygybę padauginę iš $h(x)$, gauname

$$\big(f(x)\,h(x)\big)\,u(x)+g(x)\,\big(h(x)\,v(x)\big)=h(x).$$

Pagal 7 ir 8 dalumo savybes $g(x)\mid h(x)$.

3. *Jeigu $f(x)$ ir $g(x)$ – tarpusavyje pirminiai polinomai, $h(x)$ ir $g(x)$ – taip pat tarpusavyje pirminiai, tai ir sandauga $f(x)\,h(x)$ yra tarpusavyje pirminė su $g(x)$.*

Įrodymas. Jeigu $\delta(x)\mid g(x)$, tai $f(x)$ ir $\delta(x)$ – tarpusavyje pirminia polinomai. Tarkime, kad $\delta(x)$ yra $f(x)\,h(x)$ ir $g(x)$ bendrasis daliklis. Tada $f(x)$ ir $\delta(x)$ – tarpusavyje pirminiai polinomai, o $\delta(x)\mid f(x)\,h(x)$. Pagal 2 savybę $\delta(x)\mid h(x)$. Tačiau ir $\delta(x)\mid g(x)$. Tai prieštarauja sąlygai, kad $\deg(\delta)\neq 0$.

4. *Jeigu $f(x)$ ir $g(x)$ – tarpusavyje pirminiai polinomai, tai su bet kokiais natūriniais m ir n polinomai $(f(x))^n$ ir $(g(x))^m$ yra tarpusavyje pirminiai.*

Įrodoma matematinės indukcijos metodu, remiantis 3 savybe.

Pateiksime teoremą, kuria remdamiesi galėsime rasti kelių polinomų didžiausią bendrąjį daliklį.

144 teorema. *Nelygių nuliui polinomų $f_1(x)$, …, $f_m(x)\in L[x]$ $(m\geqslant 3)$ didžiausias bendrasis daliklis egzistuoja; jis tenkina lygybę*

$$\mathrm{D}\big(f_1(x),\ \ldots,\ f_m(x)\big)=\mathrm{D}\big(\delta_{m-1}(x),\ f_m(x)\big);$$

čia

$$\delta_{m-1}(x)=D\big(f_1(x),\ \ldots,\ f_{m-1}(x)\big).$$

Įrodymas. Įrodysime teoremą, kai $m=3$.

Tarkime, kad

$$\delta(x)=\mathrm{D}\left(\delta_2(x),\ f_3(x)\right)$$

ir

$$\delta_2(x)=\mathrm{D}\left(f_1(x),\ f_2(x)\right).$$

Kadangi $\delta(x) \mid \delta_2(x)$ ir $\delta(x) \mid f_3(x)$, tai

$$\delta(x) \mid f_i(x) \quad (i=1,\ 2,\ 3). \tag{8.3}$$

Jeigu $d(x)$ yra bet kuris polinomų $f_1(x)$, $f_2(x)$, $f_3(x)$ bendrasis daliklis, tai $d(x) \mid f_1(x)$ ir $d(x) \mid f_2(x)$. Taigi $d(x) \mid f_3(x)$ ir $d(x) \mid \delta_2(x)$. Tai reiškia, kad $d(x) \mid \delta(x)$. Iš pastarojo ir iš (8.3) sąryšių išplaukia, jog $\delta(x)$ yra polinomų $f_1(x)$, $f_2(x)$, $f_3(x)$ bendrasis daliklis, kuris dalijasi iš kiekvieno tų polinomų bendrojo daliklio. Taigi $\delta(x)=\mathrm{D}(f_1(x), f_2(x), f_3(x))$.

Tarkime, kad teorema teisinga, kai $m=r$. Tuomet

$$\mathrm{D}\left(f_1(x),\ \ldots,\ f_r(x)=\mathrm{D}\left(\mathrm{D}\left(f_1(x),\ \ldots,\ f_{r-1}(x)\right),\ f_r(x)\right)\right.$$

ir

$$\mathrm{D}\left(f_1(x),\ \ldots,\ f_{r+1}(x)\right)=\mathrm{D}\left(\mathrm{D}\left(f_1(x),\ \ldots,\ f_{r-1}(x)\right),\ f_r(x),\ f_{r+1}(x)\right)=$$

$$=\mathrm{D}\left(\mathrm{D}\left(f_1(x),\ \ldots,\ f_r(x)\right),\ f_{r+1}(x)\right).$$

Taigi teorema teisinga ir tada, kai $m=r+1$.

Uždaviniai

5. Raskite polinomų $f(x)$ ir $g(x)$ didžiausią bendrąjį daliklį:

a) $f(x)=x^4-2x^3-x^2+4x-2$, $g(x)=x^3+x^2-5x+3$;

b) $f(x)=2x^6-x^4-2x^2+1$, $g(x)=6x^7-3x^5+4x^3-6x^2-2x+3$;

c) $f(x)=3x^8+9x^7+5x^6+21x^4-18x^3+10x-30$, $g(x)=2x^6+3x^5-9x^4+4x^2-18x+18$;

d) $f(x)=3x^5+6x^3+5x^2+10$, $g(x)=7x^3+7x^2-13x-13$;

e) $f(x)=3\sqrt{2}\,x^5-2\sqrt{2}\,x^4+3\pi x^3-2(6+\pi)x^2+8x$, $g(x)=\sqrt{2}\,x^5+(\sqrt{2}+\pi)x^3-4x^2+\pi x-4$;

f) $f(x)=(2-i)x^7-ix^5+(2-i)x^4+(1-i)x^3-ix^2+(1-i)$, $g(x)=3(2-i)x^6-2(1+i)x^4+(3-2i)x^2-(1-i)$.

6. Polinomų $f(x)$ ir $g(x)$ didžiausią bendrąjį daliklį $\mathrm{D}(x)$ tiesiškai išreikškite polinomais $f(x)$ ir $g(x)$, t. y. raskite tokius polinomus $u(x)$ ir $v(x)$, kad būtų teisinga lygybė $\mathrm{D}(x)=u(x)f(x)+v(x)g(x)$:

a) $f(x)=3x^6-6x^5+3x^4+x^3-3x^2+3x-1$, $g(x)=x^4-2x^3+3x^2-4x+2$;

b) $f(x)=7x^5+10x^3+3x^2-8x+6$, $g(x)=3x^3+x^2+6x+2$;

c) $f(x)=x^3+2x^2-3x-5$, $g(x)=2x^5+4x^4-3x^3-4x^2-9x-16$;

d) $f(x)=-6x^7+x^5+13x^3-5x$, $g(x)=3x^5+x^3-6x$.

7. Raskite polinomų $f(x)$, $g(x)$ ir $\varphi(x)$ didžiausią bendrąjį daliklį:

a) $f(x)=x^5+4x^3-7x^2-28$,
$g(x)=2x^5+8x^3-x^2-4$,
$\varphi(x)=x^5+3x^4+7x^3+13x^2+12x+4$;

b) $f(x)=x^3+3x^2+3x+1$,
$g(x)=6x^7-10x^5+6x^4-3x^3+5x-3$,
$\varphi(x)=2x^4-9x^2+4$.

§73. Iracionalumo trupmenos vardiklyje naikinimas

Vidurinėje mokykloje, tapačiai pertvarkant algebrinius reiškinius, kartais tenka naikinti iracionalumą vardiklyje, t. y. reiškinį

$$f(\alpha)/g(\alpha)$$

užrašyti šitaip:

$$f(\alpha)/g(\alpha)=\varphi(\alpha);$$

čia α – iracionalusis skaičius, o f, g ir φ – polinomai su racionaliaisiais koeficientais.

Pavyzdys.

$$\frac{3}{\sqrt{3}+1}=\frac{3(\sqrt{3}-1)}{(\sqrt{3}+1)(\sqrt{3}-1)}=\frac{3(\sqrt{3}-1)}{(\sqrt{3})^2-1}=\frac{3}{2}\sqrt{3}-\frac{3}{2};$$

čia

$$\alpha=\sqrt{3},\ f(\alpha)=3,\ g(\alpha)=\alpha+1,\ \varphi(\alpha)=\frac{3}{2}\alpha-\frac{3}{2},$$

$f(x)=3$ – nulinio laipsnio polinomas, $g(x)=x+1$ – pirmojo laipsnio polinomas, $\varphi(x)=\frac{3}{2}x-\frac{3}{2}$ – pirmojo laipsnio polinomas.

Jeigu $\alpha\in L$ yra algebrinis elementas lauko **L** *atžvilgiu, o $g(x)\neq O(x)$ – polinomas virš to lauko, tai reiškinys $g(\alpha)\neq O$ vadinamas iracionaliuoju reiškiniu, arba iracionalumu.*

Santykyje $f(\alpha)/g(\alpha)$ iracionalumas yra trupmenos vardiklyje. Trupmenos vardiklio iracionalumą tenka naikinti nagrinėjant lauko plėtinių konstrukcijas. Kartais išspręsti tokį uždavinį gana sudėtinga, ypač kai α yra aukšto laipsnio algebrinis elementas. Tolesnė teorema teigia, kad iracionalumą vardiklyje panaikinti galima, ir nurodo, kaip tai galima atlikti.

145 teorema. *Jeigu* $\alpha \in L$ *yra algebrinis elementas* **L** *atžvilgiu, o* $f(x)$ *ir* $g(x) \in L[x]$, $g(\alpha) \neq O$, *tai egzistuoja toks polinomas* $\varphi(x) \in L[x]$, *kurio laipsnis mažesnis už elemento* α *laipsnį ir su kuriuo teisinga lygybė*

$$f(\alpha)/g(\alpha) = \varphi(\alpha).$$

Įrodymas. Tarkime, kad $\alpha \in L$ yra algebrinis n-ojo laipsnio elementas lauko **L** atžvilgiu. Pažymėkime $p(x) \in L[x]$ žemiausio laipsnio polinomą, kurio šaknis yra α, $p(\alpha) = O$. Ir tegul $\deg(p) = n$ yra elemento α laipsnis. Polinomai $g(x)$ ir $p(x)$ – tarpusavyje pirminiai. Tuo įsitikiname tarę, kad yra nenulinio laipsnio polinomas $d(x)$, $d(x) \mid g(x)$ ir $d(x) \mid p(x)$. Tuomet

$$p(x) = d(x) p_1(x) \quad \text{ir} \quad p(\alpha) = d(\alpha) p_1(\alpha) = O.$$

Kadangi $g(x) = d(x) g_1(x)$ ir $O \neq g(\alpha) = d(\alpha) g_1(\alpha)$, tai $d(\alpha) \neq O$. Todėl $p_1(\alpha) = O$. Tai prieštarauja polinomo $p(x)$, kaip žemiausio laipsnio polinomo, kurio šaknis α, parinkimui.

Pasinaudoję $D(g(x), p(x))$ tiesine išraiška, turėsime

$$e = p(x) u(x) + g(x) v(x), \quad u(x), \quad v(x) \in L[x],$$

ir

$$e = g(\alpha) v(\alpha).$$

Todėl

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha) v(\alpha)}{g(\alpha) v(\alpha)} = f(\alpha) v(\alpha).$$

Polinomą $f(x) v(x) \in L[x]$ padaliję su liekana iš $p(x)$, gausime

$$f(x) v(x) = p(x) q(x) + \varphi(x), \quad q(x), \quad \varphi(x) \in L[x],$$

ir $\varphi(x) = O(x)$ arba $\deg(\varphi) < \deg(p)$.

Kadangi $f(\alpha) v(\alpha) = \varphi(\alpha)$, tai ir $f(\alpha)/g(\alpha) = \varphi(\alpha)$.

Sprendžiant konkretų uždavinį, reikia rasti polinomą $p(x)$ ir išraišką $e = p(x) u(x) + g(x) v(x)$. Polinomo $v(x)$ reikšmė taške α, t. y. $v(\alpha)$, ir yra tas daugiklis, iš kurio padauginus trupmenos skaitiklį ir vardiklį, jos vardiklyje iracionalumo nebelieka.

Pavyzdys. Panaikinkime iracionalumą reiškinio

$$\frac{5}{\sqrt[3]{4} - 6\sqrt[3]{2} + 1}$$

vardiklyje.

Nesunku pastebėti, kad $\sqrt[3]{4} = (\sqrt[3]{2})^2$. Vadinasi, vardiklis yra $\alpha^2 - 6\alpha + 1$ pavidalo, $\alpha = \sqrt[3]{2}$. Taigi

$$g(x) = x^2 - 6x + 1.$$

$\sqrt[3]{2}$ yra lygties $x^3-2=0$ šaknis. Todėl $p(x)=x^3-2$. Ieškosime daugiklio $v(\alpha)$. Pirmiausia reikia rasti polinomą $v(x)$. Taikome Euklido algoritmą:

$$x^3-2=g(x)(x+6)+(35x-8);\quad q_0(x)=x+6,\ r_1(x)=35x-8;$$

$$g(x)=r_1(x)\left(\frac{1}{35}\,x-\frac{202}{35^2}\right)+\left(-\frac{391}{35^2}\right);$$

$$q_1(x)=\frac{1}{35}\,x-\frac{202}{35^2},\quad r_2=-\frac{391}{35^2}.$$

Gauname

$$r_2=g(x)-r_1(x)\,q_1(x),\quad r_1(x)=p(x)-g(x)\,q_0(x).$$

$r_1(x)$ išraišką įrašome į pirmąją lygybę:

$$r_2=p(x)\left(-q_1(x)\right)+g(x)\left(1+q_0(x)\,q_1(x)\right).$$

Iš čia

$$1=p(x)\left(-\frac{1}{r_2}\,q_1(x)\right)+g(x)\left(\frac{1}{r^2}\left(1+q_0(x)\,q_1(x)\right)\right).$$

Taigi

$$v(x)=\frac{1}{r_2}\left(1+q_0(x)\,q_1(x)\right)=-\frac{1}{391}\,(35x^2+8x+13),$$

o

$$v(\alpha)=-\frac{1}{391}\,(35\sqrt[3]{4}+8\sqrt[3]{2}+13).$$

Padauginę iš to daugiklio pradinio reiškinio skaitiklį ir vardiklį, gauname

$$\frac{5}{\sqrt[3]{4}-6\sqrt[3]{2}+1}=-\frac{5}{391}\,(35\sqrt[3]{4}+8\sqrt[3]{2}+13).$$

Uždaviniai

8. Panaikinkite iracionalumą trupmenos vardiklyje:

a) $\dfrac{3\alpha+4}{5\alpha^2+6\alpha+3}$, kai $\alpha^3+3=0$;

b) $\dfrac{5\alpha-2}{\alpha^2+2\alpha+1}$, kai $\alpha^3-5=0$;

c) $\dfrac{\alpha^2+3\alpha-5}{3\alpha^3+4\alpha^2+2\alpha+1}$, kai $\alpha^4-2\alpha^2-1=0$.

9. Panaikinkite iracionalumą reiškinio vardiklyje:

a) $\dfrac{1}{\sqrt[3]{2}+2}$, b) $\dfrac{2+\sqrt[3]{2}}{3\sqrt[3]{4}-5\sqrt[3]{2}+1}$, c) $\dfrac{1}{2\sqrt[4]{3}+3\sqrt[4]{9}+2}$,

d) $\dfrac{1}{2+\sqrt[3]{3}}$, e) $\dfrac{1}{\sqrt[4]{3}-2\sqrt[4]{2}}$.

§74. Polinomų mažiausias bendrasis kartotinis

Nelygių nuliui polinomų $f_1(x), \ldots, f_m(x)$ $(m \geqslant 2)$ iš $L[x]$ *bendruoju kartotiniu* vadiname polinomą $M(x) \in L[x]$, kuris dalijasi iš polinomų $f_1(x), \ldots, f_m(x)$.

Polinomų $f_1(x), \ldots, f_m(x)$ *bendrąjį kartotinį, iš kurio dalijasi visi tų polinomų bendrieji kartotiniai*, vadiname polinomų $f_1(x), \ldots, f_m(x)$ *mažiausiu bendruoju kartotiniu* ir žymime $M(f_1(x), \ldots, f_m(x))$.

Bet kurie nenuliniai polinomai $f_1(x), \ldots, f_m(x)$ $(m \geqslant 2)$ iš $L[x]$ turi bendruosius kartotinius. Iš tikrųjų polinomas

$$\prod_{j=1}^{m} f_j(x)$$

dalijasi iš kiekvieno polinomo $f_1(x), \ldots, f_m(x)$. Jeigu $f(x)$ yra bet kuris polinomas iš $L[x]$, tai polinomas

$$f(x) \prod_{j=1}^{m} f_j(x)$$

taip pat yra polinomų $f_1(x), \ldots, f_m(x)$ bendrasis kartotinis. (Taigi *neasocijuotų bendrųjų kartotinių yra be galo daug.*) Kadangi polinomų $f_1(x), \ldots, f_m(x)$ bendrųjų kartotinių skirtumas yra tų polinomų bendrasis kartotinis, tai *polinomų* $f_1(x), \ldots, f_m(x)$ *bendrųjų kartotinių aibė yra žiedo* $\mathbf{L}[x]$ *idealas.* Iš dalybos su liekana teoremos 3 išvados išplaukia, kad žiede $\mathbf{L}[x]$ *tas idealas yra vyriausiasis.* Taigi egzistuoja toks polinomas $M(x) \in L[x]$, kad tas idealas yra $(M(x))$, t. y. kiekvienas polinomų bendrasis kartotinis dalijasi iš jų bendrojo kartotinio $M(x)$. Įrodėme, jog *egzistuoja bet kurių nelygių nuliui polinomų* $f_1(x), \ldots, f_m(x)$ *virš lauko* $\mathbf{L}$ *mažiausias bendrasis kartotinis.*

Dviejų polinomų mažiausią bendrąjį kartotinį nesunku rasti, kai žinomas jų didžiausias bendrasis daliklis.

146 teorema. *Jeigu* $f(x) \neq O(x)$, $g(x) = O(x)$ *yra polinomai virš* $\mathbf{L}$, *tai*

$$D(f(x), g(x)) \cdot M(f(x), g(x)) = f(x)\, g(x).$$

Įrodymas. Iš sąryšio $M(f, g) \mid fg$ išplaukia, kad

$$\delta_1(x) = \frac{f(x)\, g(x)}{M(f(x), g(x))} \in L[x].$$

Kadangi $f(x) \mid M(f, g)$ ir $g(x) \mid M(f, g)$, tai iš pastarosios lygybės gauname

$$f(x) = \frac{\delta_1(x)\, M(f(x), g(x))}{g(x)}, \quad g(x) = \frac{\delta_1(x)\, M(f(x), g(x))}{f(x)}.$$

Vadinasi, $\delta_1(x) \mid f(x)$ ir $\delta_1(x) \mid g(x)$.

Tarkime, jog egzistuoja toks polinomų $f(x)$ ir $g(x)$ bendrasis daliklis $d(x)$, kad $d(x)=\delta_1(x)\varphi(x)$ ir $\varphi(x)$ yra nenulinio laipsnio polinomas. Tada

$$f(x)=d(x)f_1(x)=\frac{\delta_1(x)\,\mathrm{M}\left(f(x),\ g(x)\right)}{g(x)},$$

$$g(x)=d(x)g_1(x)=\frac{\delta_1(x)\,\mathrm{M}\left(f(x),\ g(x)\right)}{f(x)}.$$

Iš tų lygybių gauname išraiškas:

$$\frac{\mathrm{M}\left(f(x),\ g(x)\right)}{g(x)}=\frac{d(x)}{\delta_1(x)}f_1(x),\quad \frac{\mathrm{M}\left(f(x),\ g(x)\right)}{f(x)}=\frac{d(x)}{\delta_1(x)}g_1(x);$$

čia

$$\varphi(x)=\frac{d(x)}{\delta_1(x)}\in L[x].$$

Iš pastarųjų išraiškų matyti, kad polinomai

$$\frac{\mathrm{M}\left(f(x),\ g(x)\right)}{g(x)}\quad\text{ir}\quad\frac{\mathrm{M}\left(f(x),\ g(x)\right)}{f(x)}$$

turi netrivialųjį daliklį $\varphi(x)$. Bet tuomet polinomas

$$\mathrm{M}_1(x)=\frac{\mathrm{M}\left(f(x),\ g(x)\right)}{\varphi(x)}\in L[x]$$

yra žemesnio laipsnio negu $\mathrm{M}(f(x),\ g(x))$ ir jis yra polinomų $f(x)$ ir $g(x)$ bendrasis kartotinis. Kadangi $\mathrm{M}(f(x),\ g(x))\mid \mathrm{M}_1(x)$, tai gauname prieštaravimą.

Taigi prielaida, kad polinomų $f(x)$ ir $g(x)$ bendrasis daliklis $d(x)$ turi tiesioginį daliklį $\delta_1(x)$, yra neteisinga. Todėl teisingas sąryšis $d(x)\mid\delta_1(x)$, kuris reiškia, kad $\delta_1(x)$ yra polinomų $f(x)$ ir $g(x)$ didžiausias bendrasis daliklis.

Išvada.

$$\mathrm{M}\left(f(x),\ g(x)\right)=\frac{f(x)\,g(x)}{\mathrm{D}\left(f(x),\ g(x)\right)}.$$

147 teorema. *Jeigu* $f_1(x),\ \ldots,f_m(x)$ $(m\geqslant 3)$ *yra nelygūs nuliui polinomai virš lauko* L, *tai*

$$\mathrm{M}\left(f_1(x),\ \ldots,f_m(x)\right)=\mathrm{M}\left(\mathrm{M}\left(f_1(x),\ \ldots,f_{m-1}(x)\right),f_m(x)\right).$$

Įrodymas. Žymėkime $\mathrm{M}(x)=\mathrm{M}\left(f_1(x),\ldots,f_m(x)\right)$, $\mathrm{M}_1(x)=\mathrm{M}(f_1(x),\ldots,f_{m-1}(x))$. Kadangi $f_j(x)\mid\mathrm{M}_1(x)$ $(j=1,\ldots,m-1)$ ir polinomų $f_1(x),\ldots,f_{m-1}(x)$ bendrųjų kartotinių aibė yra vyriausiasis idealas, generuotas polinomo $\mathrm{M}_1(x)$, tai $\mathrm{M}_1(x)\mid\mathrm{M}(x)$. Jeigu polinomas $\overline{\mathrm{M}}(x)$ yra polinomų $\mathrm{M}_1(x)$ ir $f_m(x)$ bendrasis kartotinis, tai jis yra ir polinomų $f_1(x),\ \ldots,f_m(x)$ bendrasis kartotinis. Todėl $\mathrm{M}(x)\mid\overline{\mathrm{M}}(x)$. Taigi $\mathrm{M}_1(x)\mid\mathrm{M}(x)$ ir $f_m(x)\mid\mathrm{M}(x)$. Paėmę $\overline{\mathrm{M}}(x)=\mathrm{M}\left(\mathrm{M}_1(x)\,|\,f_m(x)\right)$, gauname $\overline{\mathrm{M}}(x)\mid\mathrm{M}(x)$. Pasta-

rieji du sąryšiai reiškia, kad $M(x)=c\overline{M}(x)$ $(c\in L,\ c\neq O)$.

Remdamiesi įrodytąja teorema, galime rasti trijų ir daugiau nenulinių polinomų mažiausią bendrąjį kartotinį. Dviejų nenulinių polinomų mažiausią bendrąjį kartotinį rasime naudodamiesi 146 teoremos išvada.

Pavyzdys. Rasime $M(f, g)$, kai

$$f(x)=x^3-6x^2+11x-6,\ g(x)=3x^3+3x^2-x-5.$$

Kadangi $D\big(f(x), g(x)\big)=x-1$, tai

$$M\big(f(x), g(x)\big)=\frac{f(x)\,g(x)}{x-1}.$$

Užrašome $f(x)=(x-1)(x^2-5x+6)$. Tuomet

$$M\big(f(x), g(x)\big)=(3x^3+3x^2-x-5)(x^2-5x+6)=3x^5-12x^4+2x^3+18x^2+19x-30.$$

Uždaviniai

10. Raskite polinomų $f(x)$ ir $g(x)$ mažiausią bendrąjį kartotinį:

a) $f(x)=2x^5+4x^4+6x^3+3x^2+6x+9$,
$g(x)=x^3+x^2+x-3$;

b) $f(x)=x^5+x^4-x^3-x^2-x+1$,
$g(x)=x^4+5x^3-2x^2-9x+5$.

11. Raskite šių polinomų mažiausią bendrąjį kartotinį:

$$f(x)=2x^4+3x^3+2x+3,$$
$$g(x)=2x^5+x^4+5x^3+2x^2+x+5,$$
$$h(x)=x^4-3x^3+x-3.$$

§75. Pirminiai ir sudėtiniai polinomai. Sudėtinio polinomo išraiška pirminių polinomų sandauga

Kiekvienas polinomas $f(x)\neq O(x)$ virš lauko **L** turi trivialiųjų daliklių, t. y. jis dalijasi iš nelygių nuliui lauko **L** elementų ir iš sau asocijuotų polinomų, nes

$$f(x)=c\big(c^{-1}f(x)\big)=\big(cf(x)\big)c^{-1}\quad (c\neq O,\ c\in L).$$

Nenulinio laipsnio polinomas $p(x)\in L[x]$ vadinamas pirminiu (neskaidžiuoju) polinomu žiede **L** *[x], jei jis neturi kitų daliklių, išskyrus trivialiuosius.*

Nenulinio laipsnio polinomas $f(x)\in L[x]$ vadinamas sudėtiniu žiede $L[x]$ (skaidžiuoju), jei jis turi netrivialiųjų daliklių.

Vadinasi, jeigu polinomas $f(x)$ yra sudėtinis žiede $\mathbf{L}[x]$, tai egzistuoja tokie nenulinio laipsnio polinomai $g(x)$, $q(x) \in L[x]$, kad $f(x)=g(x)\,q(x)$. Ir atvirkščiai, jeigu $f(x)=g(x)\,q(x)$ ir $g(x)$, $q(x) \in L[x]$ yra nenulinio laipsnio polinomai, tai polinomas $f(x)$ yra sudėtinis žiede $\mathbf{L}[x]$.

Visa nenulinio laipsnio polinomų virš $\mathbf{L}$ aibė suskyla į du poaibius: pirminių polinomų ir sudėtinių polinomų aibes, neturinčias bendrų elementų.

Pavyzdžiui, visi pirmojo laipsnio polinomai $p(x)=ax+b$, $a \neq O$, $a, b \in L$, yra pirminiai žiede $\mathbf{L}[x]$.

Kalbant apie pirminius polinomus, visada reikia nurodyti, kokiame polinomų žiede jie nagrinėjami. Pasitaiko atvejų, kai tas pats polinomas žiede $\mathbf{L}[x]$ yra pirminis, o žiede $\mathbf{L}'[x]$, kai $\mathbf{L}'$ – lauko $\mathbf{L}$ viršlaukis, jau yra sudėtinis, ir atvirkščiai.

Pavyzdys. Polinomas

$$p(x)=2x^2-1$$

yra pirminis žiede $\mathbf{Q}[x]$. Kadangi

$$2x^2-1=2\left(x-\frac{\sqrt{2}}{2}\right)\left(x+\frac{\sqrt{2}}{2}\right),$$

ai žieduose $\mathbf{R}[x]$ ir $\mathbf{K}[x]$ tas polinomas jau sudėtinis. Polinomas

$$f(x)=x^4-2$$

žiede $\mathbf{K}[x]$ ir $\mathbf{R}[x]$ sudėtinis, nes

$$x^4-2=(x^2-\sqrt{2})(x^2+\sqrt{2}),$$

o žiede $\mathbf{Q}[x]$ polinomas $f(x)$ yra pirminis.

Išnagrinėsime keletą pirminių polinomų savybių.

1. *Jeigu $p(x)$ yra pirminis polinomas virš $\mathbf{L}$, o $f(x) \neq O$ (x) – bet koks polinomas virš $\mathbf{L}$, tai $p(x) \mid f(x)$ arba polinomai $f(x)$ ir $p(x)$ yra tarpusavyje pirminiai.*

Įrodymas. Tarkime, kad $\delta(x)=\mathrm{D}(p(x), f(x))$. Kadangi $\delta(x) \mid p(x)$, tai $\delta(x)=c \neq O$, arba $\delta(x)=cp(x)$. Taip pat $\delta(x) \mid f(x)$, taigi ir $p(x) \mid f(x)$.

2. *Jeigu $p(x)$ ir $q(x)$ yra pirminiai žiede $\mathbf{L}[x]$ polinomai, tai teisingas tik vienas iš teiginių: $\mathrm{D}(p(x), q(x))=e$ arba $q(x)=cp(x)$, $c \neq O$ $(p(x)$ ir $g(x)$ – tarpusavyje pirminiai arba asocijuotieji polinomai).*

Įrodymas. Ši savybė gaunama iš pirmosios savybės, pastebėjus, kad $q(x)=cp(x)$, $c \neq O$, jei $p(x) \mid q(x)$.

3. *Jeigu polinomų $f(x)$ ir $g(x)$ sandauga dalijasi iš pirminio polinomo $p(x)$, tai ir bent vienas iš dauginamųjų dalijasi iš $p(x)$.*

Įrodymas. Tarkime, kad $p(x) \mid f(x)\,g(x)$ ir $p(x) \nmid f(x)$. Tada pagal 1 savybę $\mathrm{D}(p(x), f(x))=e$, o pagal tarpusavyje pirminių polinomų 2 savybę (žr. § 72) $p(x) \mid g(x)$. Analogiškai samprotaujame ir kai $p(x) \nmid g(x)$.

4. *Kiekvienas sudėtinis žiede $\mathbf{L}[x]$ polinomas $f(x)$ turi pirminį daliklį tame žiede.*

Įrodymas. Sakykime, $g_1(x)$, $g_2(x)$, ..., $g_m(x)$, ... yra polinomo $f(x)$ tiesioginių daliklių seka. Tarę, kad ji begalinė, gausime prieštaravimą 136 teoremai. Todėl ta daliklių seka yra baigtinė. Jos paskutinis polinomas neturi tiesioginių daliklių, taigi yra pirminis.

Polinomų virš lauko žiede $\mathbf{L}[x]$, kaip ir kiekviename Euklido žiede, teisinga teorema apie skaidymą. Ją galima suformuluoti šitaip.

148 teorema. *Kiekvienas nenulinio laipsnio polinomas $f(x)$ iš $\mathbf{L}[x]$ yra arba pirminis žiede $\mathbf{L}[x]$, arba išreiškiamas pirminių tame žiede polinomų sandauga, t. y.*

$$f(x)=\prod_{j=1}^{k} p_j(x).$$

Toji išraiška yra vienintelė pirminių asocijuotųjų daugiklių, jų tvarkos ir lauko $\mathbf{L}$ vieneto daliklių tikslumu.

Pastaba. Ta teorema yra 123 teoremos (žr. § 57) išvada, nes žiedas $\mathbf{L}[x]$ – Euklido žiedas. Pateiksime tradicinį teoremos įrodymą, kad jį galėtų suprasti ir tie, kurie dėl vienos ar kitos priežasties neskaitė šeštojo skyriaus.

Įrodymas. Jeigu $f(x)$ yra pirminis polinomas, tai teorema teisinga. Taigi užtenka įrodyti teoremą, kai $f(x)$ yra sudėtinis polinomas.

Remdamiesi pirminių polinomų 4 savybe, žymėkime

$$f(x)=p_1(x)f_1(x),\ f_{j-1}(x)=p_j(x)f_j(x),$$

$p_1(x)$ ir $p_j(x)$, $j=2$, ..., – pirminiai dalikliai. Pagal 136 teoremą

$$f(x)=p_1(x)p_2(x)\ldots p_k(x).$$

Pastaroji lygybė yra polinomo $f(x)$ išraiška pirminių polinomų sandauga

Tarkime, kad gavome dvi išraiškas

$$f(x)=\prod_{j=1}^{k} p_j(x) \quad \text{ir} \quad f(x)=\prod_{j=1}^{s} q_j(x),$$

kuriose daugikliai yra pirminiai virš $\mathbf{L}$ polinomai. Lygybės

$$\prod_{j=1}^{k} p_j(x)=\prod_{j=1}^{s} q_j(x)$$

kairiojoje pusėje esantis polinomas dalijasi iš $p_1(x)$. Todėl pagal pirminių polinomų 1–3 savybes tos lygybės dešiniojoje pusėje bent vienas pirminis polinomas yra asocijuotas polinomui $p_1(x)$. Kadangi dauginamuosius galime sukeisti vietomis, tai

$$q_1(x)=c_1p_1(x).$$

Suprastinę abi puses iš $p_1(x)$, gauname lygybę

$$\prod_{j=2}^{k} p_j(x)=c_1\prod_{j=2}^{s} q_j(x).$$

Pakartoję samprotavimą $r=\min\{k, s\}$ kartų, gausime lygybes $q_j(x)=c_j p_j(x)$, $j=1, 2, \ldots, r$, ir lygybes

$$e=\left(\prod_{j=1}^{k} c_j\right) q_{k+1}(x)\ldots q_s(x), \quad \text{kai} \quad k<s,$$

$$p_{s+1}(x)\ldots p_k(x)=\prod_{j=1}^{s} c_j, \quad \text{kai} \quad k>s,$$

$$e=\prod_{j=1}^{k} c_j, \quad \text{kai} \quad k=s.$$

Pirmoji ir antroji lygybės yra neteisingi teiginiai (nulinio laipsnio polinomas lygus nenulinio laipsnio polinomui), todėl negali būti nei $k<s$, nei $k>s$. Taigi $k=s$.

Išraiškos vienatis įrodyta.

Atkreipsime dėmesį, kad teoremos įrodymas nėra konstruktyvus – nenurodo būdo skaidiniui rasti. Tačiau pačiu teiginiu gana sėkmingai remiamasi sprendžiant įvairius polinomų teorijos uždavinius.

Polinomo išraiškoje pirminių daugiklių sandauga sugrupavę vienodus daugiklius (ir galbūt pakeitę žymėjimus), gausime išraišką

$$f(x)=\prod_{j=1}^{r} (p_j(x))^{l_j},$$

kuri *vadinama polinomo* $f(x)$ *kanoniniu skaidiniu.* Pastarojoje sandaugoje jau nėra vienodų pirminių daugiklių. *Laipsnio rodikliai* $l_j \geqslant 1$ *vadinami pirminių daugiklių* $p_j(x)$ *kartotinumais.*

Polinomo $f(x)\in L[x]$ kanoniniame skaidinyje pirminiai polinomai $p_j(x)$ gali būti įvairių laipsnių. Vietoje lauko $\mathbf{L}$ imant jo plėtinius $\mathbf{L}'$, galima pasiekti (žr. § 76), kad visi pirminiai kanoninio skaidinio daugikliai virš $\mathbf{L}'[x]$ būtų pirmojo laipsnio, t. y. $f(x)\in L'[x]$ jau galima būtų išreikšti šitaip:

$$f(x)=\prod_{j=1}^{k} (a_j x+b_j)^{m_j};$$

čia $a_j\neq O$, $a_j, b_j\in L'$.

Minimalusis laukas $\mathbf{L}'$, *virš kurio polinomo* $f(x)\in L[x]$ *kanoniniame skaidinyje yra tik pirmojo laipsnio pirminiai daugikliai, vadinamas polinomo* $f(x)$ *skaidinio lauku.*

Naudodamiesi polinomų kanoniniais skaidiniais, galime rasti tų polinomų didžiausią bendrąjį daliklį ir mažiausią bendrąjį kartotinį. Sakykime,

$$f(x)=\prod_{j=1}^{r}(p_j(x))^{l_j},\quad g(x)=\prod_{j=1}^{k}(q_j(x))^{t_j}$$

yra polinomų $f(x)\neq O(x)$ ir $g(x)\neq O(x)$ kanoniniai skaidiniai. Prirašę trūkstamus daugiklius – nulinio laipsnio polinomus $(p_j(x))^0=e$ ir $(g_j(x))^0=e$), suvienodinsime abiejų polinomų išraiškas:

$$f(x)=\prod_{j=1}^{m}(p_j(x))^{l_j},\quad g(x)=\prod_{j=1}^{m}(p_j(x))^{t_j}.$$

Skaitytojui siūlome pačiam įrodyti, kad

$$\mathrm{D}(f(x),\ g(x))=\prod_{j=1}^{m}(p_j(x))^{u_j},\ u_j=\min\{l_j,\ t_j\},\quad j=1,\ 2,\ \ldots,\ m,$$

$$\mathrm{M}(f(x),\ g(x))=\prod_{j=1}^{m}(p_j(x))^{v_j},\ v_j=\max\{l_j,\ t_j\},\quad j=1,\ 2,\ \ldots,\ m.$$

Gautąsias išraiškas galima apibendrinti imant bet kurį baigtinį skaičių polinomų. Taigi šios formulės analogiškos formulėms sveikųjų skaičių didžiausiam bendrajam dalikliui ir mažiausiam bendrajam kartotiniui rasti naudojantis tų skaičių kanoniniais skaidiniais.

Pavyzdys. Jeigu

$$f(x)=(x+1)^3(x^2+2)^2(x^3+2),\ g(x)=(x-1)(x+1)^2(x^2+2)^3(x^3-2),$$

tai

$$\mathrm{D}(f(x),\ g(x))=(x+1)^2(x^2+2)^2,\ \mathrm{M}(f(x),\ y(x))=$$
$$=(x-1)(x+1)^3(x^2+2)^3(x^3+2)(x^3-2).$$

§76. Polinomo šaknies egzistavimo teorema

Esame įrodę (žr. § 68, 140 teoremą), kad kiekvienas n-ojo ($n\geqslant 1$) laipsnio polinomas $f(x)$ virš integralumo srities kiekviename jos plėtinyje turi ne daugiau kaip n šaknų. Tarkime, kad $f(x)\in\check{Z}[x]$ – koks nors konkretus polinomas. Ar egzistuoja toks integralumo srities $\check{\mathbf{Z}}$ plėtinys $\mathbf{L}$, kuriame polinomas $f(x)$ turėtų bent vieną šaknį?

Kaip įsitikinome 58 paragrafe, kiekviena integralumo sritis turi plėtinį – *santykių lauką*. Taigi $\check{Z}\subset L$ ir $f(x)\in\check{Z}[x]$, taip pat $f(x)\in L[x]$. Iš to išplaukia, kad pakanka nagrinėti tik polinomus virš lauko $\mathbf{L}$. Kadangi kiekvieną sudėtinį polinomą $f(x)\in L[x]$ galima išreikšti pirminių polinomų sandauga, o kiekvieno daugiklio šaknis yra ir polinomo šaknis, tai iškeltą klausimą galime formuluoti šitaip.

Sakykime, $p(x)$ – *pirminis polinomas virš lauko* **L**. *Ar yra toks lauko* **L** *plėtinys* **L'** ($L \subset L'$), *kuriame polinomas* $p(x)$ *turi šaknį*?

Atsakymo į tą klausimą ieškosime remdamiesi faktoržiedo sąvoka.

Jeigu $p(x) \in L[x]$, tai aibė $\{p(x)\,g(x) \mid g(x) \in L[x]\}$ yra idealas žiede **L** $[x]$. Pažymėkime

$$[r(x)]_p = \{f(x) \mid f(x) = p(x)\,q(x) + r(x)\} = \{f(x) \mid f(x) - r(x) \in (p(x))\}$$

ekvivalentumo klasę pagal sąryšį „lygsta mod $(p(x))$" žiede **L** $[x]$. Jai priklauso polinomas $r(x)$. Tokias klases vadinsime *liekanų klasėmis* moduliu $p(x)$. Sąryšis „lygsta mod $(p(x))$" smulkiau išnagrinėtas 53 paragrafe. Ten aprašyta ir žiedo faktoržiedo pagal idealą konstrukcija. Prisiminę liekanų klasių veiksmus:

$$[f(x)]_p + [g(x)]_p = [f(x) + g(x)]_p,\ [f(x)]_p\,[g(x)]_p = [f(x)\,g(x)]_p$$

ir 110 bei 111 teoremas, konstatuojame, kad *algebrinė struktūra*

$$\mathbf{L}[x]/p = \big(L[x]/(p(x)),\ +,\ \cdot\big)$$

yra laukas. Šio lauko vienetinis elementas – klasė $[e]_p$, o nulinis elementas – klasė $[O]_p = (p(x))$.

Pavyzdys. Rasime $[f]_p + [g]_p$ ir $[f]_p \cdot [g]_p$, kai

$$p(x) = x^2 - 2,\ f(x) = x^3 + 2x - 3,\ g(x) = x^7 - 7x^5 - 4x^4 + 3x^3 - 6x + 15.$$

Kadangi

$$f(x) = x\,(x^2 - 2) + (4x - 3),\ g(x) = (x^2 - 2)\,(x^5 - 5x^3 - 4x^2 - 7x - 8) + (-20x - 1),$$

tai

$$f \in [r_1]_p,\quad r_1(x) = 4x - 3.$$

$$g \in [r_2]_p,\quad r_2(x) = -20x - 1.$$

Liekanas sudėję, gauname

$$r_1(x) + r_2(x) = -16x - 4,$$

o sudauginę –

$$r_1(x) \cdot r_2(x) = -80\,(x^2 - 2) + (-104x + 3).$$

Todėl

$$[f]_p + [g]_p = [r_1]_p + [r_2]_p = [q]_p,\quad q(x) = -16x - 4,$$

$$[f]_p \cdot [g]_p = [r_1]_p \cdot [r_2]_p = [h]_p,\quad h(x) = -104x + 3.$$

149 teorema. *Jeigu* **L** *yra laukas,* $p(x)$ – *pirminis polinomas virš* **L**, *tai faktorlaukas* **L** $[x]/p$ *turi polaukį, izomorfišką laukui* **L**.

Įrodymas. Pažymėkime $\overline{L}$ aibės $L[x]/(p(x))$ poaibį:

$$\overline{L} = \{[a]_p \mid a \in L\}.$$

Tada

$$[a]_p + [b]_p = [a + b]_p \in \overline{L},\quad [a]_p \cdot [b]_p = [ab]_p \in \overline{L}.$$

Kai $a \neq O$, gauname $[a]_p \cdot [a^{-1}]_p = [e_p]$. Iš čia $[a]_p^{-1} = [a^{-1}]_p \in \overline{L}$. Todėl $\overline{\mathbf{L}} = (L, +, \cdot)$ yra lauko **L** $[x]/p$ polaukis.

Apibrėšime bijekciją φ: $L \leftrightarrow \overline{L}$ šitaip:

$$\varphi(a) = [a]_p, \quad a \in L.$$

Kadangi

$$\varphi(a+b) = [a+b]_p = [a]_p + [b]_p = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = [ab]_p = [a]_p \cdot [b]_p = \varphi(a) \cdot \varphi(b),$$

tai bijekcija φ yra izomorfizmas.

150 teorema. *Jeigu* **L** *yra laukas, o* $p(x)$ *– pirminis polinomas virš* **L**, *tai egzistuoja toks lauko* **L** *viršlaukis* **L'**, *kuriame polinomas* $p(x)$ *turi šaknį.*

Įrodymas. Tarkime, kad

$$p(x) = \sum_{j=0}^{n} c_j x^j.$$

Pažymėkime $\alpha = [x]_p$. Prisiminę klasių veiksmų savybes, gausime lygybes

$$[O]_p = \big(p(x)\big) = [p(x)]_p = \Big[\sum_{j=0}^{n} c_j x^j\Big]_p = \sum_{j=0}^{n} [c_j]_p [x]_p^j. \tag{8.4}$$

Lauko $\mathbf{L}[x]/p$ elementus $[a]_p$ $(a \in L)$ pakeitę atitinkamais elementais a, gausime aibę

$$L' = \Big(\big(L[x]/\big(p(x)\big)\big) \setminus \overline{L}\Big) \cup L,$$

t. y. aibės L viršaibį. Papildomai apibrėžę veiksmus šioje aibėje:

$$a + [f(x)]_p = [a]_p + [f(x)]_p = [a + f(x)]_p, \quad a \cdot [f(x)]_p = [a]_p \cdot [f(x)]_p = [af(x)]_p,$$

gausime algebrinę struktūrą – lauką

$$\mathbf{L'} = (L', +, \cdot),$$

t. y. lauko **L** viršlaukį. Šiame viršlaukyje pagal (8.4) formules

$$p(\alpha) = \sum_{j=0}^{n} c_j [x]_p^j = \sum_{j=0}^{n} c_j \alpha^j = [O]_p.$$

Kadangi elementas $[O]_p$ pakeistas elementu O, tai $p(\alpha) = O$, $\alpha \in L'$. Teorema įrodyta.

151 teorema. *Kiekvienas nenulinio laipsnio polinomas virš integralumo srities turi skaidinio lauką.*

Įrodymas. Tarkime, kad $\check{\mathbf{Z}}$ yra integralumo sritis, o $f(x)$ – nenulinio laipsnio polinomas. Kai **L** – integralumo srities $\check{\mathbf{Z}}$ santykių laukas, tai ir $f(x) \in L[x]$. Pagal 148 teoremą virš šio lauko turėsime skaidinį

$$f(x) = \prod_{j=1}^{k} \big(p_j(x)\big)^{l_j}.$$

Pagal 150 teoremą egzistuoja laukas $\mathbf{L}_1$ ($L \subset L_1$), kuriame polinomas $p_1(x)$ turi šaknį l_1 ($l_1 \in L_1$). Tada

$$f(x) = (x - l_1) f_1(x), \quad f_1(x) \in L_1[x].$$

Toliau nagrinėsime polinomą $f_1(x)$. Pagal tą pačią teoremą gausime lauką $\mathbf{L}_2$ ($L \subset L_1 \subset L_2$), virš kurio

$$f(x) = (x - l_1)(x - l_2) f_2(x).$$

Analogiškai po n žingsnių ($n = \deg f(x)$) gausime laukus $\mathbf{L} \subset \mathbf{L}_1 \subset \ldots \subset \mathbf{L}_n$, $l_i \in L_i$, $i = 1, \ldots, n$, ir

$$f(x) = c(x - l_1)(x - l_2) \ldots (x - l_n), \quad c \in L, \ c \neq O.$$

Minimalus lauko $\mathbf{L}_n$ polaukis L_f, kuriam priklauso $l_1, \ldots, l_n$, yra polinomo $f(x)$ skaidinio laukas.

Pavyzdžiai. Polinomas $f(x) = x^2 - 2$ turi šaknį $\sqrt{2} \in \mathbf{Q}(\sqrt{2})$. Antroji jo šaknis yra $-\sqrt{2} \in \mathbf{Q}(\sqrt{2})$. Taigi to polinomo skaidinio laukas yra $\mathbf{Q}(\sqrt{2})$.

Analogiškai polinomo $x^2 + 1$ šaknys i ir $-i$ priklauso laukui $\mathbf{Q}(i)$. Tas laukas ir yra polinomo $x^2 + 1$ skaidinio laukas.

§77. Polinomų virš nulinės charakteristikos lauko išvestinės ir jų taikymai

Laikysime, kad pagrindinis laukas $\mathbf{L}$, virš kurio nagrinėsime polinomus, turi nulinę charakteristiką.

Kadangi polinomas yra reiškinys, tai jo išvestinė polinomų teorijoje apibrėžiama formaliai nusakant, koks polinomas yra to polinomo išvestinė.

n-ojo laipsnio ($n \geqslant 1$) polinomo

$$f(x) = \sum_{j=0}^{n} a_j x^j \in L[x]$$

išvestine, žymima $f'(x)$, vadinamas $n-1$-ojo laipsnio polinomas

$$f'(x) = \sum_{j=1}^{n} j a_j x^{j-1} \in L[x].$$

Nulinio laipsnio polinomo $f(x) = c \neq O$ išvestine vadinamas nulinis polinomas: $c' = O(x)$.

Polinomo k-oji išvestinė yra $k-1$-osios išvestinės išvestinė ($k = 2, 3, \ldots, n$). Ji žymima $f^{(k)}(x)$.

Iš apibrėžimo išplaukia:

$$f^{(2)}(x)=\sum_{j=2}^{n} j(j-1)a_j x^{j-2},$$

$$f^{(k)}(x)=\sum_{j=k}^{n} j(j-1)\ldots\big(j-(k-1)\big)a_j x^{j-k}, \quad k=2,\ \ldots,\ n,$$

$$\big(f^{(n)}(x)=n!\,a_n\big),\ f^{(k)}(x)=0, \quad \text{kai} \quad k>n.$$

Kai lauko **L** charakteristika lygi nuliui ir $n\geqslant 1$, iš $a_n\neq O$ išplaukia $na_n\neq O$. Todėl n-ojo laipsnio polinomo $f(x)$ išvestinė $f'(x)$ yra $n-1$-ojo laipsnio polinomas. Analogiškai, kai $k\leqslant n$, gauname $n(n-1)\ldots(n-(k-1))a_n\neq O$. Todėl virš nulinės charakteristikos lauko n-ojo laipsnio polinomo k-oji išvestinė ($k=1,\ \ldots,\ n$) yra $n-k$-ojo laipsnio polinomas virš to paties lauko. Aukštesnės negu n-osios eilės išvestinės yra lygios nuliui.

Pavyzdys. Apskaičiuokime visas polinomo

$$f(x)=3x^6+5x^5-6x^4-3x^3+2x^2-x+3$$

išvestines:

$$f^{(1)}(x)=18x^5+25x^4-24x^3-9x^2+4x-1,$$
$$f^{(2)}(x)=90x^4+100x^3-72x^2-18x+4,$$
$$f^{(3)}(x)=360x^3+300x^2-144x-18,$$
$$f^{(4)}(x)=1080x^2+600x-144,$$
$$f^{(5)}(x)=2160x+600,$$
$$f^{(6)}(x)=2160,\ f^{(k)}(x)=0, \quad \text{kai} \quad k>6.$$

Kai žinomos polinomo f ir visų jo išvestinių reikšmės viename lauko **L** taške, galima apskaičiuoti polinomo reikšmę bet kuriame to lauko taške. Tam tikslui naudojamės formule, vadinama anglų matematiko *Teiloro* vardu (B. Taylor, 1685–1731).

152 teorema. (Teiloro formulė.) *Jeigu $f(x)\in L[x]$ yra n-ojo laipsnio polinomas, tai su bet kokiais z ir l iš L teisinga lygybė*

$$f(l+z)=\sum_{k=0}^{n}\frac{1}{k!}f^{(k)}(l)\,z^k;$$

čia $f^{(0)}(l)=f(l)$.

Įrodymas. Žinome, kad

$$f^{(k)}(l)=\sum_{j=k}^{n} j(j-1)\ldots\big(j-(k-1)\big)a_j l^{j-k}, \quad k=1,\ \ldots,\ n.$$

Kadangi

$$f(l+z)=\sum_{j=0}^{n} a_j(l+z)^j,$$

tai, naudodamiesi lygybėmis

$$(l+z)^0=1,\ (l+z)^j=\sum_{k=0}^{j} C_j^k l^{j-k} z^k,\quad j=1,\ \ldots,\ n,$$

gauname

$$f(l+z)=\sum_{j=0}^{n} a_j \sum_{k=0}^{j} C_j^k l^{j-k} z^k.$$

Pastarojoje išraiškoje sukeitę sumavimo tvarką, turime

$$f(l+z)=\sum_{k=0}^{n} \left(\sum_{j=k}^{n} C_j^k a_j l^{j-k}\right) z^k.$$

Remdamiesi lygybėmis

$$C_j^k=\frac{1}{k!}\, j(j-1)\ldots\big(j-(k-1)\big),$$

gauname

$$\sum_{j=k}^{n} C_j^k a_j l^{j-k}=\frac{1}{k!}\sum_{j=k}^{n} j(j-1)\ldots\big(j-(k-1)\big)\, a_j l^{j-k}=\frac{1}{k!}\, f^{(k)}(l).$$

Taigi

$$f(l+z)=\sum_{k=0}^{n} \frac{1}{k!}\, f^{(k)}(l)\, z^k,\quad z\in L.$$

Tai ir reikėjo įrodyti.

Teiloro formulę galime užrašyti ir kitaip. Pažymėkime $x=z+l$. Tada $z=x-l$. Įrašę išraišką į formulę, gauname

$$f(x)=\sum_{k=0}^{n} \frac{1}{k!}\, f^{(k)}(l)\,(x-l)^k.$$

Pastaroji išraiška dar vadinama *polinomo* $f(x)$ *skleidiniu dvinario* $x-l$ *laipsniais*. Norint rasti tą skleidinį, reikia apskaičiuoti polinomo ir jo išvestinių reikšmes taške l. Aišku, kad šis skleidinys dvinario $x-l$ laipsniais sutampa su 67 paragrafe nagrinėtu skleidiniu (žr. 138 teoremą):

$$f(x)=\sum_{k=0}^{n} r_k (x-l)^k.$$

Taigi ir

$$\frac{1}{k!}\, f^{(k)}(l)=r_k,\quad k=0,\ 1,\ \ldots,\ n.$$

Iš šios lygybės gauname formules

$$f^{(k)}(l)=k!\ r_k, k=0,\ 1,\ \ldots,\ n;$$

čia r_k – liekanos, gaunamos nuosekliai dalijant $f(x)$ iš dvinario $x-l$, nepilnąjį dalmenį iš dvinario $x-l$ ir t. t. Jas, kaip įsitikinome 67 paragrafe, patogu skaičiuoti naudojantis Hornerio schema.

Pavyzdys. Polinomą $f(x)=3x^6+5x^5-6x^4+2x^2-1$ išskleiskime dvinario $x+3$ laipsniais ir apskaičiuokime $f^k(-3)$, $k=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$.

Kadangi $x-l=x+3$, tai $l=-3$. Nuosekliai dalijame iš dvinario $x+3$:

l	3	5	−6	0	2	0	−1
−3	3	−4	6	−18	56	−168	$503=r_0$
−3	3	−13	45	−153	515	$-1713=r_1$	
−3	3	−22	101	−456	$1883=r_2$		
−3	3	−31	194	$-1038=r_3$			
−3	3	−40	$314=r_4$				
−3	3	$-49=r_5$					
−3	$3=r_6$						

Gauname

$$f(x)=3(x+3)^6-49(x+3)^5+314(x+3)^4-1038(x+3)^3+$$
$$+1883(x+3)^2-1713(x+3)+503;$$
$$f^{(0)}(-3)=f(-3)=503,\quad f^{(1)}(-3)=-1713,\quad f^{(2)}(-3)=2\cdot 1883,$$
$$f^{(3)}(-3)=6(-1038),\quad f^{(4)}(-3)=24\cdot 314,\quad f^{(5)}(-3)=120(-49),$$
$$f^{(6)}(-3)=720\cdot 3=2160.$$

Polinomų sumos ir sandaugos išvestinės randamos pagal formules, žinomas iš matematinės analizės. Jas čia įrodysime remdamiesi polinomo išvestinės apibrėžimu.

153 teorema.

a) $\big(f(x)+g(x)\big)'=f'(x)+g'(x)$,

b) $\big(f(x)\,g(x)\big)'=f'(x)\,g(x)+f(x)\,g'(x)$

Įrodymas. Tarkime, kad

$$f(x)=\sum_{j=0}^{n} a_j x^j, \quad g(x)=\sum_{l=0}^{m} b_l x^l.$$

a) Turime

$$f(x)+g(x)=\sum_{k=0}^{N} (a_k+b_k)\, x^k;$$

čia $N=\max\{n, m\}$ ir $a_k=O$, kai $k>n$, $b_k=O$, kai $k>m$. Remdamiesi polinomo išvestinės apibrėžimu, gauname

$$\big(f(x)+g(x)\big)'=\sum_{k=1}^{N} k\,(a_k+b_k)\, x^{k-1}=$$

$$=\sum_{k=1}^{n} k a_k x^{k-1}+\sum_{k=1}^{m} k b_k x^{k-1}=f'(x)+g'(x).$$

b) Kadangi

$$f(x)\,g(x)=\sum_{k=0}^{n+m}\Big(\sum_{j+l=k} a_j b_l\Big)\, x^k,$$

tai pagal polinomo išvestinės apibrėžimą

$$\big(f(x)\,g(x)\big)'=\sum_{k=1}^{n+m} k\Big(\sum_{j+l=k} a_j b_l\Big)\, x^{k-1}. \tag{8.5}$$

Išdiferencijavę atskirai kiekvieną polinomą, turime

$$f'(x)=\sum_{j=1}^{n} j a_j x^{j-1} \quad \text{ir} \quad g'(x)=\sum_{l=1}^{m} l b_l x^{l-1}.$$

Sudauginę gauname

$$f'(x)\,g(x)=\sum_{k=1}^{n+m}\Big(\sum_{j+l=k} j a_j b_l\Big)\, x^{k-1}$$

ir

$$f(x)\,g'(x)=\sum_{k=1}^{n+m}\Big(\sum_{j+l=k} l a_j b_l\Big)\, x^{k-1}.$$

Sudėję pastarąsias lygybes, randame

$$f'(x)g(x)+f(x)g'(x)=\sum_{k=1}^{n+m}\Big(\sum_{j+l=k}(j+l)a_jb_l\Big)x^{k-1}=$$

$$=\sum_{k=1}^{n+m}k\Big(\sum_{j+l=k}a_jb_l\Big)x^{k-1}.$$

Sugretinę pastarąją ir (8.5) lygybes, gauname antrąjį teoremos tvirtinimą.

Pirmąjį teoremos tvirtinimą apibendrinti bet kokiam baigtiniam dėmenų skaičiui paliekame skaitytojui. Apibendrinsime tik antrąją teoremos dalį.

154 teorema.

$$\Big(\prod_{k=1}^{m}f_k\Big)'=\sum_{k=1}^{m}f_k^{(1)}\prod_{j\neq k}f_j\quad(m>2).$$

Atskiru atveju, kai $f_k=f$, $k=1, 2, \ldots, m$, *teisinga ši formulė*:

$$(f^m)'=mf'f^{m-1}.$$

Įrodymas. Remdamiesi 131 teorema, gauname

$$\Big(\prod_{k=1}^{r}f_k\Big)'=\Big(f_r\prod_{k=1}^{r-1}f_k\Big)'=f_r'\prod_{k=1}^{r-1}f_k+f_r\Big(\prod_{k=1}^{r-1}f_k\Big)'.$$

Teoremos tvirtinimas yra teisingas, kai $r=2$. Tarę, kad

$$\Big(\prod_{k=1}^{r-1}f_k\Big)'=\sum_{k=1}^{r-1}f_k'\prod_{j\neq k}f_k,$$

iš pirmosios lygybės gauname

$$\Big(\prod_{k=1}^{r}f_k\Big)'=f_r'\prod_{j=1}^{r-1}f_j+f_r\sum_{k=1}^{r-1}f_k'\prod_{j\neq k}f_j=\sum_{k=1}^{r}f_k'\prod_{j\neq k}f_j.$$

Iš matematinės indukcijos principo išplaukia, kad teorema teisinga.

Uždaviniai

12. Polinomą $f(x)$ išskleiskite $x-l$ laipsniais. Raskite polinomo ir jo visų išvestinių reikšmes taške l:

a) $f(x)=4x^3-3x^2+5x-8$, $l=-1$;

b) $f(x)=3x^3+4x^2+2x-3$, $l=i$;

c) $f(x)=3x^6+6x^5-x^4+3x^3-15x-7$, $l=-2$;

d) $f(x)=6x^5-4x^4+3x^2+5x=7$, $l=\frac{2}{3}$;

e) $f(x)=(3+i)x^3+(1-i)x^2+(2-3i)x-4+5i$, $l=1-i$.

§78. Polinomo kartotinių daugiklių atskyrimas

Jeigu polinomo $f(x)$ virš lauko $\mathbf{L}$ su nuline charakteristika kanoninėje išraiškoje

$$f(x)=\prod_{j=1}^{s}(p_j(x))^{l_j}$$

visų pirminių polinomų $p_j(x)$, $j=1, \ldots, s$, kartotinumai l_j lygūs 1, tai $f(x)$ *vadinamas polinomu, neturinčiu kartotinių daugiklių.* Jeigu bent vieno pirminio daugiklio kartotinumas l_j didesnis už 1, tai polinomas $f(x)$ turi *kartotinių daugiklių.*

Kaip jau minėjome, nėra algoritmo polinomo pirminiams dalikliams rasti. Tačiau yra metodas (algoritmas) polinomo kartotiniams dalikliams rasti.

Kanoniniame skaidinyje visų k-ojo kartotinumo pirminių daugiklių sandaugą pažymėję $g_k(x)$, $k=1, 2, \ldots, m$, $m=\max\{l_1, \ldots, l_s\}$, gausime

$$f(x)=g_1(x)(g_2(x))^2\ldots(g_m(x))^m.$$

Jeigu polinomo visų pirminių daliklių $p_j(x)$ kartotinumai l_j lygūs 1, tai $m=1$ ir $f(x)=g_1(x)$. Polinomas $f(x)$ tuo atveju neturi kartotinių daugiklių. Jeigu yra $l_j>1$, tai pastarojoje $f(x)$ išraiškoje bus daugiklių $g_j(x)$ su $j>1$. Daugikliai $g_j(x)$, $j=1, 2, \ldots, m$, *vadinami j-ojo kartotinumo daugikliais.* Mokysimės juos rasti. Tuo tikslu prireiks vienos pirminio kartotinio daugiklio savybės.

155 teorema. *Jeigu polinomas $f(x)$ turi l-ojo, $l\geqslant 1$, kartotinumo pirminį daliklį $p(x)$, tai jo išvestinėje to pirminio daliklio kartotinumas yra $l-1$.*

Įrodymas. Kadangi $f(x)=(p(x))^l g(x)$ ir $p(x)\nmid g(x)$, tai

$$f'(x)=(p(x))^{l-1}(lp'(x)g(x)+p(x)g'(x)).$$

$p(x)$ – pirminis polinomas, taigi $p(x)\nmid p'(x)g(x)$, o $p(x)\mid p(x)g'(x)$. Todėl ir $lp'(x)g(x)+p(x)g'(x)$ nesidalija iš $p(x)$.

Išvada. *Jeigu polinomo $f(x)$ kanoninis skaidinys yra*

$$f(x)=\prod_{j=1}^{m}(p_j(x))^{l_j},$$

tai $f'(x)=\left(\prod_{j=1}^{m}(p_j(x))^{l_j-1}\right)\varphi(x)$ *ir* $\varphi(x)$ *nesidalija iš nė vieno pirminio polinomo* $p_j(x)$, $j=1, \ldots, m$.

Remdamiesi šia išvada, įrodysime tokį teiginį.

Polinomo $f(x)$ kartotinius daugiklius galima (efektyviai) rasti.

Įrodymas. Pasinaudoję išraiška

$$f(x)=g_1(x)\left(g_2(x)\right)^2\left(g_3(x)\right)^3\ldots\left(g_m(x)\right)^m,$$

suformuluotąja išvada ir dviejų polinomų didžiausio bendrojo daliklio formule, kai žinomi tų polinomų skaidiniai, gausime šias išraiškas:

$$\delta_1(x)=\mathrm{D}\left(f(x),\ f'(x)\right)=g_2(x)\left(g_3(x)\right)^2\ldots\left(g_m(x)\right)^{m-1},$$
$$\delta_2(x)=\mathrm{D}\left(\delta_1(x),\ \delta_1'(x)\right)=g_3(x)\left(g_4(x)\right)^2\ldots\left(g_m(x)\right)^{m-2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\delta_{m-1}(x)=\mathrm{D}\left(\delta_{m-2}(x),\ \delta_{m-2}'(x)\right)=g_m(x),$$
$$\delta_m(x)=\mathrm{D}\left(\delta_{m-1}(x),\ \delta_{m-1}'(x)\right)=e.$$

Iš tų išraiškų lengvai gauname lygybes

$$\varphi_1(x)=\frac{f(x)}{\delta_1(x)}=g_1(x)\,g_2(x)\ldots g_m(x);\quad \varphi_2(x)=\frac{\delta_1(x)}{\delta_2(x)}=g_2(x)\ldots g_m(x);$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi_{m-1}(x)=\frac{\delta_{m-2}(x)}{\delta_{m-1}(x)}=g_{m-1}(x)\,g_m(x),\quad \varphi_m(x)=\frac{\delta_{m-1}(x)}{\delta_m(x)}=g_m(x).$$

Iš pastarųjų lygybių išplaukia

$$g_k(x)=\frac{\varphi_k(x)}{\varphi_{k+1}(x)},\quad k=1,\ 2,\ \ldots,\ m-1,\ \text{ir}\ g_m(x)=\varphi_m(x).$$

Taigi didžiausias daugiklių $g(x)$ kartotinumas yra m, m – toks natūrinis skaičius, kad $\deg(\delta_j)>0$, $j=1,\ 2,\ \ldots,\ m-1$, ir $\deg(\delta_m)=0$. Kadangi polinomo $f(x)$ kartotinio daugiklio $g_j(x)$ kiekviena šaknis yra polinomo $f(x)$ j-ojo kartotinumo šaknis, tai teisingas šitoks teiginys.

Nenulinio laipsnio polinomas $f(x)$ virš **L** *neturi kartotinių šaknų, kai jo ir jo išvestinės didžiausias bendrasis daliklis yra nulinio laipsnio polinomas, t. y.*

$$\delta_1(x)=\mathrm{D}\left(f(x),\ f'(x)\right)=c.$$

Polinomo $f(x)$ kartotinių daugiklių radimo algoritmą galime aprašyti šitaip:

1) *randame polinomus* $\delta_1(x),\ \delta_2(x),\ \ldots,\ \delta_{m-1}(x),\ \delta_m(x)=c$:

$$\delta_1(x)=\mathrm{D}\left(f(x),\ f'(x)\right),\quad \delta_k(x)=\mathrm{D}\left(\delta_{k-1}(x),\ \delta_{k-1}'(x)\right),\quad k=2,\ \ldots,\ m,$$

2) ieškome polinomų $\varphi_1(x),\ \varphi_2(x),\ \ldots,\ \varphi_m(x)$:

$$\varphi_1(x)=\frac{f(x)}{\delta_1(x)},\quad \varphi_k(x)=\frac{\delta_{k-1}(x)}{\delta_k(x)},\quad k=2,\ \ldots,\ m,$$

3) *daugiklius* $g_k(x)$, $k=1,\ \ldots,\ m$, *randame iš lygybių*

$$g_k(x)=\frac{\varphi_k(x)}{\varphi_{k+1}(x)},\quad k=1,\ 2,\ \ldots,\ m-1,\ g_m(x)=\varphi_m(x).$$

Pažymėsime, kad skaičiavimo procesas kartais gali būti gana ilgas, nes didžiausių bendrųjų daliklių $\delta_1(x),\ \ldots,\ \delta_m(x)$ tenka ieškoti taikant Euklido algoritmą.

Pavyzdys. Rasime polinomo

$$f(x)=x^7-x^6-10x^5+6x^4+25x^3-17x^2-16x+12$$

kartotinius daugiklius.

1) Taikydami Euklido algoritmą, gauname

$$\delta_1(x)=x^3-3x+2,$$
$$\delta_2(x)=\mathrm{D}(\delta_1, \delta_1')=x-1,$$
$$\delta_3(x)=1.$$

Kadangi $\delta_3(x)=1$, tai polinomas $f(x)$ turi 3-ojo kartotinumo daugiklių.

2) Randame $\varphi_1(x)$, $\varphi_2(x)$, $\varphi_3(x)$:

$$\varphi_1(x)=x^4-x^3-7x^2+x+6, \quad \varphi_2(x)=x^2+x-2, \quad \varphi_3(x)=x-1.$$

3) Gauname

$$g_1(x)=x^2-2x-3, \quad g_2(x)=x+2, \quad g_3(x)=x-1.$$

Taigi

$$f(x)=(x^2-2x-3)(x+2)^2(x-1)^3.$$

Iš tokios išraiškos lengvai randame polinomo šaknis:

$$l_1=l_2=l_3=1, \; l_5=l_4=-2, \; l_6=3, \; l_7=-1.$$

Iš polinomo kartotinės šaknies apibrėžimo išplaukia: jeigu polinomas turi kartotinę šaknį, tai jis turi ir kartotinį daugiklį. Todėl, *atskyrę kartotinius daugiklius ,galime spręsti paprastesnį uždavinį, t. y. ieškoti šaknies polinomo, neturinčio kartotinių šaknų.* Jeigu $\delta_1(x)=c$, tai polinomas $f(x)$ neturi kartotinių daugiklių. Taigi, kai $\delta_1(x)\neq c$, galime rasti polinomo kartotinius daugiklius ir ieškoti jų šaknų, kurios yra ir paties polinomo šaknys, be to, tos šaknys tokio pat kartotinumo kaip ir atitinkamo daugiklio kartotinumas.

Uždaviniai

13. Nustatykite, ar šie polinomai turi kartotinių šaknų:

a) $x^5+2x^4-x^3-4x^2-8x+4$;
b) $3x^4-18x^3+26x^2+6x-9$;
c) $8x^5-8x^4+2x^3+12x^2-12x+3$;
d) $2x^6-6x^5+2x^4-3x^2-9x-3$.

14. Atskirkite polinomų kartotinius daugiklius ir, kur įmanoma, raskite polinomų šaknis:

a) $x^5-3x^4+4x^3-12x^2+4x-12$;
b) $x^6-4x^5-2x^4-32x^3-59x^2-44x-12$;
c) $4x^7+24x^6+36x^5-40x^4-135x^3-42x^2+108x+72$;
d) $48x^5+80x^4+40x^3-5x-1$;
e) $x^6+2\sqrt{2}x^5-4\sqrt{2}x^3-4x^2$.

15. Įrodykite, kad l yra polinomo $f(x)$ s-ojo kartotinumo šaknis tada ir tik tada, kai

$$f(l)=f^{(1)}(l)=\ldots=f^{(s-1)}(l)=0 \quad \text{ir} \quad f^{(s)}(l)\neq 0.$$

16. Parinkite p, q ir r taip, kad polinomas

$$f(x)=x^4+px^3+qx^2+rx+1$$

turėtų ne mažesnio kaip 3-ojo kartotinumo šaknį -1.

§79. Polinominių trupmenų laukas

Integralumo sritis $\check{Z}[x_1, \ldots, x_n]$, kaip ir kiekviena integralumo sritis, turi savo santykių lauką, kurį žymėsime $\check{Z}(x_1, \ldots, x_n)$. Priminsime to lauko struktūrą.

Polinomų $f(x_1, \ldots, x_n)$ ir $g(x_1, \ldots, x_n) \neq O$ virš integralumo srities $\check{Z}$ santykį

$$\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$$

vadiname n kintamųjų polinomine trupmena.

Laukas

$$\check{Z}(x_1, \ldots, x_n) = \left(\left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \;\middle|\; f, g \in \check{Z}[x_1, \ldots, x_n],\ g \neq O \right\},\ +,\ \cdot \right)$$

vadinamas *polinominių trupmenų lauku.*

Primename, kad polinominių trupmenų laukas yra integralumo srities — polinomų žiedo $\check{Z}[x_1, \ldots, x_n]$ minimalusis viršlaukis (žr. 126 teoremą).

Smulkiau nagrinėsime vieno kintamojo polinominių trupmenų lauką

$$L(x) = \left(\left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x),\ g(x) \in L(x),\ g(x) \neq O(x) \right\},\ +,\ \cdot \right).$$

Žinome, kad

$$\frac{f(x)}{g(x)} = \frac{h(x)}{k(x)},$$

kai $f(x)\,k(x) = g(x)\,h(x)$. Be to, jeigu $f_1(x)$ ir $g_1(x) \neq O(x)$, o $\delta(x) = D(f_1(x), g_1(x))$, tai $f_1(x) = \delta(x) f(x)$, $g_1(x) = \delta(x)\, g(x)$ ir $D(f(x), g(x)) = e$. Todėl su kiekviena polinomine trupmena teisingos lygybės

$$\frac{f_1(x)}{g_1(x)} = \frac{\delta(x) f(x)}{\delta(x) g(x)} = \frac{f(x)}{g(x)};$$

čia $f(x)$ ir $g(x)$ — tarpusavyje pirminiai polinomai.

Polinominė trupmena $f(x)/g(x)$, kurios skaitiklis $f(x)$ ir vardiklis $g(x)$ yra tarpusavyje pirminiai polinomai, vadinama nesuprastinamąja trupmena.

Atliktas samprotavimas rodo, kad *kiekviena nenulinė vieno kintamojo polinominė trupmena lygi nesuprastinamai trupmenai.*

Polinominė trupmena, kurios skaitiklio laipsnis mažesnis už vardiklio laipsnį, vadinama taisyklingąja trupmena.

Pagal dalybos su liekana teoremą su bet kokiais polinomais $f(x)$ ir $g(x) \neq O(x)$ virš **L** teisinga išraiška

$$f(x)=g(x)\,q(x)+r(x),$$

kurioje $r(x)=O(x)$, arba $\deg(r)<\deg(g)$, ir polinomai $q(x)$ ir $r(x)$ yra vienintelei. Be to, jeigu $f(x)$ ir $g(x)$ yra tarpusavyje pirminiai polinomai, tai $q(x)$ ir $r(x)$ taip pat tarpusavyje pirminiai.

Todėl teisingas šitoks teiginys: *kiekvieną polinominę nesuprastinamąją trupmeną vienintelių būdu galima išreikšti šitaip*:

$$\frac{f(x)}{g(x)}=q(x)+\frac{r(x)}{g(x)};$$

čiai $q(x)\in L[x]$, o $\frac{r(x)}{g(x)}$ — *nesuprastinama taisyklingoji trupmena.*

Pavyzdys. Trupmena $\frac{x^2-6}{x^3-3x+2}$ yra taisyklinga ir nesuprastinama, o

$$\frac{x^2+2x-1}{3x-5}=\left(\frac{1}{3}x+\frac{3}{2}\right)+\frac{13}{6x-10}.$$

156 teorema. *Jeigu*

$$g(x)=\prod_{j=1}^{s}\left(p_j(x)\right)^{l_j}$$

yra polinomo $g(x)$ *kanoninis skaidinys žiede* **L** $[x]$, *tai kiekvieną nesuprastinamą taisyklingąją trupmeną*

$$\frac{f(x)}{g(x)}\in L(x)$$

vienintelių būdu galima išreikšti nesuprastinamų taisyklingųjų trupmenų suma:

$$\frac{f(x)}{g(x)}=\sum_{j=1}^{s}\frac{f_j(x)}{\left(p_j(x)\right)^{l_j}}.$$

Įrodymas. Tarkime, kad $g(x)=g_1(x)\,g_2(x)$ ir $\mathrm{D}(g_1, g_2)=e$. Tada egzistuoja tokie polinomai $u(x)$, $v(x)\in L[x]$, kad

$$e=g_1(x)\,u(x)+g_2(x)\,v(x).$$

Pažymėję $f_2(x)=u(x)f(x)$, $f_1(x)=v(x)f(x)$, gauname

$$\frac{f(x)}{g(x)}=\frac{f_1(x)}{g_1(x)}+\frac{f_2(x)}{g_2(x)}.$$

Kadangi $\deg(u) < \deg(g_2)$ ir $\deg(v) < \deg(g_1)$, tai $\deg(ug_1) < \deg(g_1g_2)$ ir $\deg(vg_2) < \deg(g_1g_2)$. Todėl $\deg(f_1) < \deg(g_1)$ ir $\deg(f_2) < \deg(g_2)$. Iš to išplaukia, kad

$$\frac{f_1(x)}{g_1(x)} \quad \text{ir} \quad \frac{f_2(x)}{g_2(x)}$$

yra taisyklingosios polinominės trupmenos.

Jeigu bet kuri iš jų būtų suprastinama, pavyzdžiui,

$$\frac{f_1(x)}{g_1(x)} = \frac{k(x)}{h(x)},$$

čia $\deg(h) < \deg(g_1)$, tai būtų teisingos lygybės:

$$\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{k(x)}{h(x)} + \frac{f_2(x)}{g_2(x)} = \frac{k(x)\,g_2(x) + h(x)\,f_2(x)}{h(x)\,g_2(x)},$$

ir trupmena

$$\frac{f(x)}{g(x)}$$

būtų suprastinama, nes $\deg(hg_2) < \deg(g_1g_2) = \deg(g)$.

Taigi

$$\frac{f_1(x)}{g_1(x)}, \quad \frac{f_2(x)}{g_2(x)}$$

yra nesuprastinamos taisyklingosios trupmenos.

Kai

$$g(x) = \prod_{j=1}^{s} \left(p_j(x)\right)^{l_j},$$

užrašę

$$g_1(x) = \left(p_1(x)\right)^{l_1}, \quad g_2(x) = \prod_{j=2}^{s} \left(p_j(x)\right)^{l_j},$$

gauname

$$\frac{f(x)}{g(x)} = \frac{f_1(x)}{\left(p_1(x)\right)^{l_j}} + \frac{h_2(x)}{g_2(x)}.$$

Analogiškai

$$\frac{h_2(x)}{g_2(x)} = \frac{f_2(x)}{\left(p_2(x)\right)^{l_j}} + \frac{h_3(x)}{g_3(x)}, \quad g_3(x) = \prod_{j=3}^{s} \left(p_j(x)\right)^{l_j}.$$

Pakartoję tą samprotavimą $s-1$ kartą, gausime išraišką

$$\frac{f(x)}{g(x)} = \sum_{j=1}^{s} \frac{f_j(x)}{\left(p_j(x)\right)^{l_j}},$$

kurioje

$$\frac{f_j(x)}{(p_j(x))^{l_j}}, \quad j=1, 2, \ldots, s,$$

yra nesuprastinamos taisyklingosios polinominės trupmenos.

Įrodysime, kad pastaroji išraiška yra vienintelė. Tarkime, jog yra dar ir kita išraiška

$$\frac{f(x)}{g(x)}=\sum_{j=1}^{s}\frac{d_j(x)}{(p_j(x))^{l_j}}.$$

Iš pirmosios išraiškos panariui atėmę antrąją, gauname lygybę

$$\sum_{j=1}^{s}\frac{h_j(x)}{(p_j(x))^{l_j}}=O(x); \tag{8.6}$$

čia $h_j(x)=f_j(x)-d_j(x)$, $j=1, \ldots, s$. Aišku, kad $p_j(x) \nmid h_j(x)$.

Tą lygybę dauginame iš

$$\theta_1(x)=(p_1(x))^{l_1-1}(p_2(x))^{l_2}\ldots(p_s(x))^{l_s}$$

ir gauname

$$\frac{u_1(x)}{p_1(x)}+u_2(x)+\ldots+u_s(x)=O(x);$$

čia

$$u_j(x)=h_j(x)\,\theta_1(x)/(p_j(x))^{l_j}\in L[x], \quad j=2, \ldots, s,$$

ir

$$u_1(x)=h_1(x)\prod_{j=2}^{s}(p_j(x))^{l_j}.$$

Kai $h_1(x)\neq O(x)$, polinomas $u_1(x)$ nesidalija iš $p_1(x)$. Tada

$$\frac{u_1(x)}{p_1(x)}=u_1'(x)+\frac{u_1''(x)}{p_1(x)},$$

ir

$$\frac{u_1''(x)}{p_1(x)}$$

yra nesuprastinama taisyklingoji trupmena. Taigi nesuprastinamos taisyklingosios polinominės trupmenos

$$\frac{u_1''(x)}{p_1(x)}$$

ir polinomų $u_1'(x)$, $u_2(x)$, ..., $u_3(x)$ suma lygi nuliui. Kadangi to negali būti, tai $u_1(x)=O(x)$, t. y. $h_1(x)=O(x)$.

(8.6) išraiškos paskutinės lygybės abi puses dauginame iš

$$(p_1(x))^{l_1}\ldots(p_{j-1}(x))^{l_{j-1}}(p_j(x))^{l_j-1}(p_{j+1}(x))^{l_{j+1}}\ldots(p_s(x))^{l_s}$$

ir, analogiškai samprotaudami, gauname

$$h_j(x) = O(x), \quad j = 1, 2, \ldots, s.$$

Polinominė trupmena, kurios vardiklis yra pirminio polinomo $p(x)$ laipsnis, o skaitiklio laipsnis žemesnis už $p(x)$ laipsnį, vadinama paprasčiausiąja polinomine trupmena.

Įrodysime teoremą apie trupmenos išraišką paprasčiausiųjų trupmenų suma.

157 teorema. *Kiekvieną nesuprastinamą taisyklingąją trupmeną, kurios vardiklis yra pirminio žiede* **L** $[x]$ *polinomo laipsnis,*

$$\frac{h(x)}{(p(x))^l} \in L(x)$$

vieninteliu būdu galima išreikšti šitaip:

$$\frac{h(x)}{(p(x))^l} = \sum_{j=1}^{l} \frac{q_j(x)}{(p(x))^j};$$

čia polinomų $q_j(x)$ laipsniai žemesni už polinomo $p(x)$ laipsnį ($j = 1, 2, \ldots, l$).

Įrodymas. Remdamiesi dalybos su liekana teorema, gauname:

$$h(x) = p(x)^{l-1} q_1(x) + r_1(x),$$
$$r_1(x) = p(x)^{l-2} q_2(x) + r_2(x),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_{l-2}(x) = p(x)\, q_{l-1}(x) + r_{l-1}(x), \quad g_l(x) = r_{l-1}(x).$$

Kadangi $\deg(h) < \deg(p^l)$, tai iš tų lygybių ir sandaugos laipsnio savybės išplaukia $\deg(q_j) < \deg(p)$ ($j = 1, \ldots, l-1$) ir $\deg(r_{l-1}) < \deg(p)$. Taigi

$$h(x) = \sum_{j=1}^{l} (p(x)^{l-j} q_j(x)$$

ir

$$\frac{h(x)}{(p(x))^l} = \sum_{j=1}^{l} \frac{q_j(x)}{(p(x))^j}.$$

Ta išraiška vienintelė, nes polinomai $q_1(x), \ldots, q_{l-1}(x)$ ir $q_l(x) = r_{l-1}(x)$ pagal dalybos su liekana teoremą nustatomi vienareikšmiškai.

Iš 156 ir 157 teoremų išplaukia šitokia išvada: *nesuprastinamosios trupmenos išraiška*

$$\frac{f(x)}{g(x)} = q(x) + \sum_{t=1}^{s} \sum_{j=1}^{l_t} \frac{q_j^{(t)}(x)}{(p_t(x))^j}, \quad \textit{kai } g(x) = \prod_{t=1}^{s} (p_t(x))^{l_t},$$

yra vienintelė.

Pavyzdys. Išreikšime paprasčiausiųjų trupmenų suma polinominę trupmeną

$$\frac{f(x)}{g(x)}=\frac{4x^2+3x+2}{2x^3+x^2-4x-3}.$$

Kadangi $g(x)=(x+1)^2(2x-3)$, tai, remiantis suformuluotąja išvada,

$$\frac{f(x)}{g(x)}=\frac{A}{x+1}+\frac{B}{(x+1)^2}+\frac{C}{2x-3}.$$

Rasime skaičius A, B, C. Tuo tikslu sudedame užrašytąsias trupmenas ir gautosios trupmenos skaitiklį prilyginame polinomui $f(x)$. Taigi

$$A(x+1)(2x-3)+B(2x-3)+C(x+1)^2=4x^2+3x+2.$$

Atlikę veiksmus, gauname lygybę

$$x^2(2A+C)+x(-A+2B+2C)+(-3A-3B+C)=4x^2+3x+2.$$

Skaičius A, B, C randame iš lygčių

$$\begin{aligned} 2A \quad\quad + C&=4,\\ -A+2B+2C&=3,\\ -3A-3B+C&=2. \end{aligned}$$

Tos lygčių sistemos sprendinys yra $\left(\frac{19}{25}, -\frac{3}{5}, \frac{62}{25}\right)$. Taigi

$$\frac{4x^2+3x+2}{2x^3+x^2-4x-3}=\frac{19}{25(x+1)}-\frac{3}{5(x+1)^2}+\frac{62}{25(2x-3)}.$$

Uždaviniai

17. Išreikškite lauko $R(x)$ trupmenas paprasčiausiųjų trupmenų suma:

a) $\frac{2x-1}{x^2-4x+4}$; b) $\frac{3x^2-6x+7}{2x^3-18x^2+54x-54}$;

c) $\frac{3x^4-6x^3-x^2-3x-2}{x^5+2x^3+3x^2+6}$; b) $\frac{2x^4-10x^3+7x^2+4x+3}{x^5-2x^3+2x^2-3x+2}$.

Kelių kintamųjų polinomai

§80. Pirminiai ir sudėtiniai virš integralumo srities polinomai

Šiame paragrafe nagrinėsime n ($n \geqslant 1$) kintamųjų polinomus virš integralumo srities $\check{Z}$ su vienetu e.

Žiedo $\check{Z}[x_1, \ldots, x_n]$ *nenulinio laipsnio polinomą* $p(x_1, \ldots, x_n)$ *vadiname pirminiu tame žiede, jei jis neturi tiesioginių daliklių.*

Nenulinio laipsnio polinomą, turintį tiesioginių daliklių, vadiname sudėtiniu.

75 paragrafe nagrinėjome vieno kintamojo pirminius ir sudėtinius polinomus virš lauko **L**. Kadangi **L** $[x]$ yra Euklido žiedas, tai tame žiede teisingas šitoks teiginys: *kiekvienas sudėtinis polinomas vieninteliu būdu išreiškiamas pirminių polinomų sandauga.*

Polinomo išraiškos pirminių polinomų sandauga klausimą čia aptarsime bendresniu atveju. Tarkime, kad $\check{Z}$ yra integralumo sritis (Euklido žiedas), kurios kiekvienas sudėtinis elementas vieninteliu būdu išreiškiamas pirminių elementų sandauga. Sakysime trumpai: *integralumo srityje* $\check{Z}$ *teisinga skaidymo pirminiais daugikliais teorema.* Jeigu žiede teisinga sudėtinio elemento išraiškos pirminiais daugikliais teorema, tai tos srities kiekvienas baigtinis nenulinis elementų rinkinys turi didžiausią bendrąjį daliklį ir nenulinių elementų rinkinys turi mažiausią bendrąjį kartotinį, kurie nustatomi vieneto daliklio tikslumu.

Kai integralumo srityje $\check{Z}$ teisinga skaidymo pirminiais daugikliais teorema, tada kiekvieną nenulinį polinomą $f(x) \in \check{Z}[x]$ galima užrašyti šitaip:

$$f(x) = df_1(x);$$

čia $d \in \check{Z}$ – polinomo $f(x)$ koeficientų didžiausias bendrasis daliklis, o polinomo $f_1(x)$ koeficientų didžiausias bendrasis daliklis yra vienetinis elementas.

Nenulinio laipsnio polinomą $f(x)$ *virš* $\check{Z}$, *kurio koeficientų didžiausias bendrasis daliklis yra vienetinis elementas, vadiname primityviuoju polinomu.*

1 Gauso lema. *Dviejų primityviųjų polinomų iš* $\check{Z}[x]$ *sandauga yra primityvusis polinomas.*

Įrodymas. Tarkime, kad

$$f(x)=\sum_{j=0}^{n} a_j x^j, \quad D(a_0, a_1, \ldots, a_n)=e,$$

$$g(x)=\sum_{j=0}^{m} b_j x^j, \quad D(b_0, b_1, \ldots, b_m)=e.$$

Tada

$$f(x)g(x)=\sum_{k=0}^{n+m} c_k x^k;$$

čia

$$c_k=\sum_{j+l=k} a_j b_l, \quad k=0, 1, \ldots, n+m.$$

Tarkime, kad pirminis elementas $p\in\check{Z}$ yra $c_0, c_1, \ldots, c_{n+m}$ bendrasis daliklis ir

$$p\nmid a_i,\ p\mid a_j\ (j<i);\ p\nmid b_t,\ p\mid b_l\ (l<t).$$

Tuomet

$$c_{i+t}=a_i b_t+\sum_{j=0}^{i-1} a_j b_{i+t-j}+\sum_{l=0}^{t-1} a_{i+t-l} b_l.$$

Kadangi $p\nmid a_i$ ir $p\nmid b_t$, o p – pirminis elementas, tai $p\nmid a_i b_t$. Bet abi sumos dalijasi iš p pagal i ir t parinkimą. Todėl $p\nmid c_{i+m}$. Pastarasis sąryšis prieštarauja p parinkimui. Taigi $D(c_0, c_1, \ldots, c_{n+m})=e$. Tai reiškia, kad $f(x)\,g(x)$ yra primityvusis polinomas.

Iš 1 Gauso lemos išplaukia, kad kelių *polinomų iš* $\check{Z}[x]$ *sandauga yra primityvusis polinomas tada ir tik tada, kai dauginamieji yra primityvūs polinomai.*

Norint įrodyti teiginį, pakanka pastebėti, kad tuo atveju, kai dauginamojo $f(x)$ koeficientai turi bendrąjį daliklį d, sandaugos $f(x)\,g(x)$ visi koeficientai irgi turi tą patį bendrąjį daliklį.

158 teorema. *Jeigu* $\check{Z}$ *yra integralumo sritis su vienetu* e, *kurioje teisinga skaidymo pirminiais daugikliais teorema, o* $\mathbf{L}$ *– jos santykių laukas, tai kiekvieną nenulinio laipsnio polinomą* $f(x)$ *iš* $L[x]$ *galima užrašyti šitaip*:

$$f(x)=cf_1(x);$$

čia $c\in L$, $f_1(x)$ *– primityvusis polinomas iš* $\check{Z}[x]$, *nustatomas vienareikšmiškai vieneto daliklių tikslumu. Polinomas* $f(x)$ *yra pirminis žiede* $\mathbf{L}[x]$ *tada ir tik tada, kai* $f_1(x)\in\check{Z}[x]$ *– pirminis žiede* $\check{Z}[x]$.

Įrodymas. Kiekvienas elementas iš L yra šio pavidalo:

$$\frac{a}{b},\ b\neq O,\ a,\ b\in\check{Z}.$$

Kai polinomo

$$f(x)=\sum_{j=0}^{n} a_j x^j,\quad n\geqslant 1,$$

koeficientai yra lauko **L** elementai, tada

$$a_j=\frac{c_j}{b_j},\ b_j\neq 0,\ c_j,\ b_j\in\check{Z},\quad j=0,\ 1,\ \ldots,\ n\ (a_n\neq O)$$

(kai $a_j=O$, galime laikyti $c_j=O$, $b_j=e$).

Paėmę $\mathrm{M}=\mathrm{M}(b_0,\ b_1,\ \ldots,\ b_n)$, gauname

$$\frac{c_j}{b_j}=\frac{e}{\mathrm{M}}\,c_j\mathrm{M}_j,\quad \mathrm{M}_j\in\check{Z}.$$

Pažymėję $d=\mathrm{D}(c_0\mathrm{M}_0,\ \ldots,\ c_n\mathrm{M}_n)$, turime

$$c_j\mathrm{M}_j=dl_j,\ l_j\in\check{Z},\quad j=0,\ 1,\ \ldots,\ n,$$

ir

$$\mathrm{D}(l_0,\ l_1,\ \ldots,\ l_n)=e.$$

Todėl, paėmę $c=\frac{d}{\mathrm{M}}$, gauname

$$f(x)=c\sum_{j=0}^{n} l_j x^j=cf_1(x).$$

Lieka įrodyti, kad polinomas $f_1(x)\in\check{Z}[x]$ yra vienintelis vieneto daliklių tikslumu. Tarkime, kad $f(x)=\bar{c}f_2(x)$, $\bar{c}\in L$ ir $f_2(x)$ yra primityvusis polinomas iš $\check{Z}[x]$. Tada

$$cf_1(x)=\bar{c}f_2(x).$$

Tarę, kad

$$\bar{c}=\frac{d_1}{h},\ d_1,\ h\in\check{Z},$$

gauname

$$dhf_1(x)=d_1\mathrm{M}f_2(x);$$

čia $dh\in\check{Z}$, $d_1\mathrm{M}\in\check{Z}$. Kadangi polinomai $f_1(x)$ ir $f_2(x)$ yra primityvūs, tai iš pastarosios lygybės išplaukia, kad jų koeficientai gali skirtis tik vieneto dalikliu.

Įrodysime antrąją teoremos dalį.

Jeigu polinomas

$$f(x)=cf_1(x)$$

yra sudėtinis žiede $\mathbf{L}[x]$, tai polinomas $f_1(x)$ taip pat sudėtinis tame žiede, t. y.

$$f_1(x)=g(x)h(x).$$

Remdamiesi pirmąja įrodymo dalimi, gauname

$$g(x)=c_1g_1(x),\quad h(x)=c_2h_1(x);$$

čia c_1, $c_2\in L$, $g_1(x)$ ir $h_1(x)$ – primityvieji polinomai iš $\check{Z}[x]$. Todėl

$$f_1(x)=c_1c_2g_1(x)h_1(x).$$

Kadangi $f_1(x)$ yra primityvus, $g_1(x)$ ir $h_1(x)$ – taip pat primityvūs, tai c_1c_2 yra vieneto daliklis.

Taigi

$$f_1(x)=g_2(x)h_1(x).$$

Jeigu polinomas $f_1(x)$ išskaidomas žiede $\check{\mathbf{Z}}[x]$, tai polinomas $f(x)$ juo labiau išskaidomas žiede $\mathbf{L}[x]$.

Taigi teorema įrodyta.

159 teorema. *Jeigu $\check{\mathbf{Z}}$ yra integralumo sritis su vienetu e, kurioje kiekvienas sudėtinis elementas vieninteliu būdu išreiškiamas pirminių elementų sandauga, tai n kintamųjų polinomų žiede $\check{\mathbf{Z}}[x_1, \ldots, x_n]$ kiekvienas nenulinio laipsnio polinomas yra arba pirminis tame žiede, arba išreiškiamas pirminių tame žiede polinomų sandauga vieninteliu būdu (neatsižvelgiant į asocijuotuosius daugiklius ir daugiklių tvarką).*

Įrodymas. Taikysime matematinės indukcijos metodą.

Kai $n=1$, polinomą $f(x_1)\in\check{Z}[x_1]$ pagal 148 teoremą vieninteliu būdu išreiškiame pirminių žiede $\mathbf{L}[x_1]$ polinomų sandauga:

$$f(x_1)=\prod_{j=1}^{s}p_j(x_1);$$

čia $\mathbf{L}$ – integralumo srities $\check{\mathbf{Z}}$ santykių laukas.

Iš 158 teoremos išplaukia, kad

$$p_j(x_1)=c_jq_j(x_1),\quad c_j\in L,$$

ir $q_j(x_1)$, $j=1, \ldots, s$, yra primityvusis polinomas iš $\check{Z}[x_1]$. Taigi

$$f(x_1)=\prod_{j=1}^{s}\left(c_jq_j(x_1)\right)=c_1\ldots c_s\prod_{j=1}^{s}q_j(x_1).$$

Kadangi pagal 158 teoremą $f(x_1)=cf_1(x_1)$, $c\in L$, ir $f_1(x_1)$ – primityvusis polinomas iš $\check{Z}[x_1]$, tai sandauga $c_1\ldots c_s$ nuo c gali skirtis tik vieneto dalikliu, todėl $a=c_1\ldots c_s\in\check{Z}$. Iš 158 teoremos išplaukia, kad polinomai $q_j(x_1)$, $j=1, \ldots, s$, yra pirminiai žiede $\check{\mathbf{Z}}[x_1]$ ir išraiška

$$f(x_1)=a\prod_{j=1}^{s}q_j(x_1)$$

yra vienintelė.

Tarkime, kad teorema teisinga, kai $n=m$ $(m \geqslant 1)$.
Ši prielaida reiškia, kad žiede

$$\check{Z}[x_1, \ldots, x_m]$$

teisinga skaidymo pirminiais daugikliais teorema.
Kadangi

$$\check{Z}[x_1, \ldots, x_m, x_{m+1}] = \check{Z}[x_1, \ldots, x_m][x_{m+1}]$$

ir žiedas $\check{Z}[x_1, \ldots, x_m]$ pagal prielaidą tenkina teoremos sąlygas, tai, pakartoję pirmosios įrodymo dalies samprotavimus, įsitikiname, jog teorema teisinga ir kai $n=m+1$.
Taigi teorema teisinga su kiekvienu n.
Beje, nors ir įrodėme, kad polinomą išskaidyti galima, tačiau nepateikėme jokio būdo skaidiniui rasti. Aišku, vidurinėse mokyklose daugianariai skaidomi remiantis įrodytąja teorema.
Nėra bendro metodo ne tik sudėtinio polinomo išraiškai pirminių polinomų sandauga rasti, bet nėra ir metodo, kuriuo galėtume patikrinti, ar tam tikras polinomas virš integralumo srities yra pirminis, ar sudėtinis. Yra žinomas požymis, vadinamas Eizenšteino kriterijumi, kuriuo remiantis galima patikrinti, ar vieno kintamojo polinomas yra pirminis. Prieš formuluodami tą požymį, pateiksime dar vieną Gauso lemą.
Tarkime, kad $\check{Z}$ yra integralumo sritis, kurioje teisinga teorema apie skaidymą, ir $\mathbf{L}$ – jos santykių laukas.

2 Gauso lema. *Jeigu polinomas* $f(x) \in \check{Z}[x]$ *yra sudėtinis virš* $\mathbf{L}$, *tai jis yra sudėtinis ir virš* $\check{Z}$.

Įrodymas. Tarkime, kad $f(x)=f_1(x) f_2(x)$, $f_1(x)$, $f_2(x) \in L[x]$. Pagal 158 teoremą $f_1(x)=c_1 g(x)$ ir $f_2(x)=c_2 h(x)$, c_1, $c_2 \in L$, $g(x)$, $h(x) \in \check{Z}[x]$, yra primityvieji polinomai. Tada

$$f(x)=c_1 c_2 g(x) h(x).$$

Pagal 1 Gauso lemą polinomas $g(x) h(x)$ yra primityvus. Kadangi $f(x) \in \check{Z}[x]$, tai ir $c_1 c_2 \in \check{Z}$. Pažymėję $k(x)=c_1 c_2 g(x)$, gauname

$$f(x)=k(x) h(x), \quad k(x), \quad h(x) \in \check{Z}[x].$$

Iš lemos išplaukia tokia išvada: *jeigu polinomas su sveikaisiais koeficientais yra sudėtinis virš racionaliųjų skaičių lauko, tai jis yra sudėtinis ir virš sveikųjų skaičių žiedo.*

160 teorema (Eizenšteino kriterijus). *Jeigu polinomo*

$$f(x)=\sum_{j=0}^{n} a_j x^j$$

virš Euklido žiedo $\check{Z}$ *vyriausiasis koeficientas nesidalija iš pirminio elemento* p, *visi kiti koeficientai dalijasi iš* p, *o laisvasis narys nesidalija iš* p^2, *tai tas polinomas yra pirminis žiede* $\check{Z}[x]$ *(kartu ir žiede* $\mathbf{Q}_{\check{Z}}[x]$*).*

Įrodymas. Tarkime, kad $f(x)=h(x)\,k(x)$, $h(x)$ ir $k(x)$ pagal 2 Gauso lemą yra polinomai, kurių koeficientai — žiedo $\mathbf{Z}$ elementai,

$$h(x)=\sum_{l=0}^{m} b_l x^l, \quad k(x)=\sum_{r=0}^{s} c_r x^r.$$

Tada

$$a_j=\sum_{l+r=j} b_l c_r, \quad j=0,\ 1,\ \ldots,\ m+s=n.$$

Pagal teoremos sąlygą $p \mid a_0$ ir $p^2 \nmid a_0$. Todėl $p \mid b_0 c_0$ ir $p^2 \nmid b_0 c_0$, t. y. arba $p \mid b_0$ ir $p \nmid c_0$, arba $p \mid c_0$ ir $p \nmid b_0$. Nagrinėsime pirmąjį atvejį (antrasis nagrinėjamas analogiškai).

Ne visi polinomo $h(x)$ koeficientai dalijasi iš p ($p \nmid b_m$, nes priešingu atveju $a_n=b_m c_s$ dalytųsi iš p). Tarkime, jog t yra toks, kad $p \mid b_l$, $l<t$, $p \nmid b_t$. Tada

$$a_t=b_t c_0+\sum_{\substack{l+r=t,\\ r\neq 0}} b_l c_r$$

taip pat nesidalija iš p. Tai prieštarauja teoremos sąlygai. Vadinasi, teoremos tvirtinimas teisingas.

Iš tos teoremos išplaukia šitokia išvada: *egzistuoja bet kurio laipsnio pirminiai žiede* $\mathbf{Q}[x]$ *polinomai su sveikaisiais (kartu ir su racionaliaisiais) koeficientais.*

Pavyzdžiai. 1. Polinomas $5x^6-6x^5+9x^3-15x^2+21$ yra pirminis žiede $\mathbf{Z}[x]$, nes $3 \nmid 5$, visi kiti koeficientai dalijasi iš $p=3$, o 21 nesidalija iš 3^2.

2. Polinomas $g(x)=\frac{4}{7}x^4-\frac{6}{5}x^2-\frac{7}{3}x+\frac{1}{15}$ pirminis žiede $\mathbf{Q}[x]$, nes $g(x)=\frac{1}{105}(60x^4-126x^2-245x+7)=\frac{h(x)}{105}$, o polimomas $h(x)$ tenkina Eizenšteino kriterijų, kai $p=7$.

Užduviniai

1. Suformuluokite ir įrodykite Eizenšteino kriterijų bet kokioje integralumo srityje, kurioje teisinga sudėtinio elemento skaidymo teorema.

2. Patikrinkite, ar pirminiai virš sveikųjų skaičių žiedo šie polinomai:

a) $x^5-10x^4+5x^2+35$; b) x^n+p, $n\in\mathbf{N}$;

c) $x^n+px^{n-1}+\ldots+px+p$, p — pirminis skaičius.

§81. Polinomo reiškimas formų suma. Polinomo leksikografinė išraiška

n kintamųjų polinomo $f(x_1,\ \ldots,\ x_n)$ nario

$$ax_1^{j_1}\ldots x_n^{j_n}$$

laipsnis lygus sumai $j_1+\ldots+j_n$. Kadangi skirtingų neneigiamų skaičių sumos gali būti lygios, tai polinomo f kelių, o atskiru atveju ir visų narių laipsniai gali būti lygūs.

Pavyzdys. Polinomo

$$3x_1x_2x_3-4x_1^3+7x_1^2x_3-10x_2x_3^2$$

visų narių laipsniai lygūs 3. Polinomo

$$\sum_{j=1}^{n}\sum_{i=1}^{n}a_{ij}x_ix_j$$

visų narių laipsniai lygūs 2.

n kintamųjų polinomas, kurio visų narių laipsniai lygūs m, vadinamas m-ojo laipsnio forma.

Pavyzdžiui, nulinio laipsnio forma yra žiedo $\check{Z}$ elementas. Pirmojo laipsnio forma yra

$$\sum_{j=1}^{n}a_jx_j,$$

m-ojo laipsnio forma – polinomas:

$$\sum_{j_1+\ldots+j_n=m}a_{j_1\ldots j_n}x_1^{j_1}\ldots x_n^{j_n};$$

čia sumuojama pagal tuos $j_1, \ldots, j_n$, kurių suma lygi m, t. y. $j_1+\ldots+j_n=m$, ir su kuriais $a_{j_1\ldots j_n}\neq O$.

161 teorema. *Kiekvieną n kintamųjų polinomą galima išreikšti formų suma.*

Įrodymas. Išraiškoje

$$f(x_1, \ldots, x_n)=\sum_{j_1\ldots j_n}a_{j_1\ldots j_n}x_1^{j_1}\ldots x_n^{j_n},$$

kurioje sumuojama pagal tuos indeksus $j_1, \ldots, j_n$, su kuriais $a_{j_1\ldots j_n}\neq O$, pakeitę sumavimo tvarką, gauname

$$f(x_1, \ldots, x_n)=\sum_{m}\Big(\sum_{j_1+\ldots+j_n=m}a_{j_1\ldots j_n}x_1^{j_1}\ldots x_n^{j_n}\Big).$$

Tai ir reiškia teoremos tvirtinimą.

Keičiant vietomis polinomo $f(x_1, \ldots, x_n)$ normaliosios išraiškos narius, gaunamas jam lygus polinomas. Sutvarkysime polinomo narius leksikografiškai.

Narys

$$ax_1^{j_1}\ldots x_n^{j_n},\ a\neq O,$$

vadinamas leksikografiškai vyresniu (arba tiesiog vyresniu) už narį

$$bx_1^{l_1}\ldots x_n^{l_n},$$

kai yra toks numeris k, $1\leqslant k\leqslant n$, *su kuriuo* $j_i=l_i$, $i<k$, $j_k>l_k$.

Priešingu atveju vyresniu laikomas antrasis narys.

Norint nustatyti, kuris iš dviejų narių yra vyresnis, reikia palyginti jų kintamojo x_1 laipsnius. Vyresnis yra tas narys, kurio kintamojo x_1 laipsnis didesnis. Jeigu x_1 laipsniai lygūs, tai reikia lyginti tų narių kintamojo x_2 laipsnius ir t. t. Jeigu lyginamų narių kintamųjų $x_1, \ldots, x_{k-1}$ laipsniai sutampa, tai vyresnis tas narys, kurio kintamojo x_k, $k=1, 2, \ldots, n$, laipsnis didesnis. *Taip visus polinomo narius galime išdėstyti eilės tvarka. Gausime polinomo išraišką, vadinamą leksikografine. Pirmasis tos išraiškos narys vadinamas vyriausiuoju polinomo nariu.*

Pavyzdys. Polinomą

$$f(x_1, x_2, x_3)=3x_1+4x_1x_2-6x_3+5x_1^2x_3^2-6x_1x_3+2x_3^2-4x_1^4$$

leksikografiškai užrašome šitaip:

$$f(x_1, x_2, x_3)=-4x_1^4+5x_1^2x_3^2+4x_1x_2-6x_1x_3+3x_1+2x_3^2-6x_3.$$

162 teorema. *Polinomų sandaugos vyriausiasis narys lygus dauginamųjų vyriausiųjų narių sandaugai.*

Įrodymas. Teoremą įrodysime dviejų polinomų sandaugai. Kai dauginamųjų daugiau kaip 2, teorema lengvai įrodoma matematinės indukcijos metodu.

Tarkime, kad

$$f(x_1, \ldots, x_n)=ax_1^{m_1}\ldots x_n^{m_n}+f_1(x_1, \ldots, x_n),$$

$$g(x_1, \ldots, x_n)=bx_1^{l_1}\ldots x_n^{l_n}+g_1(x_1, \ldots, x_n)$$

ir $ax_1^{m_1}\ldots x_n^{m_n}$, $bx_1^{l_1}\ldots x_n^{l_n}$ yra atitinkamai polinomo f ir polinomo g vyriausieji nariai. Tai reiškia, kad kiekvienam polinomo f_1 nariui $a_1x_1^{j_1}\ldots x_n^{j_n}$ egzistuoja toks s, $1\leqslant s\leqslant n$, kad $m_i=j_i$, $i<s$, $m_s>j_s$, ir panašiai kiekvienam polinomo g_1 nariui $b_1x_1^{k_1}\ldots x_n^{k_n}$ egzistuoja toks t, $1\leqslant t\leqslant n$, kad $l_i=k_i$, $i<t$, $l_t>k_t$.

Sudauginę polinomus, gauname

$$fg(x_1, \ldots, x_n)=abx_1^{m_1+l_1}\ldots x_n^{m_n+l_n}+ax_1^{m_1}\ldots x_n^{m_n}g_1(x_1, \ldots, x_n)+$$

$$+bx_1^{l_1}\ldots x_n^{l_n}f_1(x_1, \ldots, x_n)+f_1g_1(x_1, \ldots, x_n).$$

Kiekvienas sandaugos $ax_1^{m_1}\ldots x_n^{m_n}g_1(x_1, \ldots, x_n)$ narys yra

$$ab_1x_1^{m_1+k_1}\ldots x_n^{m_n+k_n}$$

pavidalo ir $m_i+k_i=m_i+l_i$, kai $i<t$, bet $m_t+k_t<m_t+l_t$. Kiekvienas sandaugos $bx_1^{l_1}\ldots x_n^{l_n}f_1(x_1, \ldots, x_n)$ narys užrašomas šitaip:

$$a_1 bx_1^{l_1+j_1}\ldots x_n^{l_n+j_n},$$

o $l_i+j_i=l_i+m_i$, kai $i<s$, bet $l_s+j_s<l_s+m_s$. Kiekvienas sandaugos fg narys yra

$$a_1 b_1 x_1^{j_1+k_1}\ldots x_n^{j_n+k_n}$$

pavidalo ir $j_i+k_i=m_i+l_i$, kai $i<\min\{s, t\}=r$, bet $j_r+k_r<m_r+l_r$. Tai ir rodo teoremos tvirtinimą.

Uždaviniai

3. Šiuos polinomus išreikškite formų suma:

a) $3+2x_1^3-6x_2^3+5x_1x_2^3-7x_1^2x_2^2+11x_1^3x_2^2+13x_1^4x_2^3+17x_1^2x_2^3$;
b) $4x_1-8x_2+9x_3+15-14x_1x_2^5-13x_1^3x_2x_3^3+19x_1x_2x_3^4+x_1^8-x_2^4-7x_3^7-13x_1^2x_2^2x_3^3$;
c) $x_1-6x_1^2+13x_1^3-3x_1x_2+4x_1x_2x_3-5x_2-18+13x_2^2-27x_1x_2x_3^2+$
$+16x_1x_2^2x_3-x_2^5+3x_3+4x_1^3-6x_2^3-7x_3^5$.

4. Įrodykite, kad homogeninių polinomų sandauga yra homogeninis polinomas.
5. Įrodykite, kad formų sandauga yra forma.
6. Trečiojo uždavinio polinomus sutvarkykite leksikografiškai.

§82. Simetriniai polinomai

n kintamųjų polinomas $s(x_1, \ldots, x_n)$ *virš* $\check{\mathbf{Z}}$ *vadinamas simetriniu, jei su kiekvienu skaičių* 1, 2, ..., *n kėliniu* $i_1, \ldots, i_n$

$$s(x_1, \ldots, x_n)=s(x_{i_1}, \ldots, x_{i_n}).$$

Pavyzdys. $x_1^2+x_2^2-x_3^2$, $3x_1x_2-x_1-x_2$ ir $x_1^k+x_2^k+\ldots+x_n^k$ su kiekvienu $k\geqslant 1$ yra simetriniai virš $\mathbf{Z}$ trijų, dviejų ir n kintamųjų polinomai.

163 teorema. *Simetrinių virš integralumo srities* $\check{\mathbf{Z}}$ *polinomų aibė yra žiedas.*

Įrodymas. Užtenka įrodyti (žr. 90 teoremą), kad simetrinių polinomų skirtumas ir sandauga yra simetriniai polinomai. Tarkime, kad

$$s_1(x_1, \ldots, x_n) \quad \text{ir} \quad s_2(x_1, \ldots, x_n)$$

yra simetriniai virš $\check{\mathbf{Z}}$ polinomai. Kadangi su kiekvienu kėliniu $i_1, \ldots, i_n$ teisingi sąryšiai

$$s_1(x_1, \ldots, x_n)-s_2(x_1, \ldots, x_n)=s_1(x_{i_1}, \ldots, x_{i_n})-s_2(x_{i_1}, \ldots, x_{i_n}),$$

$$s_1(x_1, \ldots, x_n)\cdot s_2(x_1, \ldots, x_n)=s_1(x_{i_1}, \ldots, x_{i_n})\cdot s_2(x_{i_1}, \ldots, x_{i_n}),$$

tai teorema teisinga.

Aišku, kad *simetrinių virš* $\check{Z}$ *polinomų žiedas yra polinomų žiedo* $\check{Z}[x_1, \ldots, x_n]$ *požiedis.*

Simetriniai polinomai

$$\sigma_k(x_1, \ldots, x_n) = \sum_{1 \leqslant j_1 < \ldots < j_k \leqslant n} x_{j_1} \ldots x_{j_k}, \quad k = 1, \ldots, n,$$

vadinami pagrindiniais n kintamųjų simetriniais polinomais. (Čia sumuojama pagal visus derinius po k elementų iš n.)

Pavyzdys. Išrašysime visus 1, 2, 3 kintamųjų pagrindinius simetrinius polinomus.
1. $n=1$: $\sigma_1(x_1)=x_1$.
2. $n=2$: $\sigma_1(x_1, x_2)=x_1+x_2$, $\sigma_2(x_1, x_2)=x_1x_2$.
3. $n=3$: $\sigma_1(x_1, x_2, x_3)=x_1+x_2+x_3$,
$\sigma_2(x_1, x_2, x_3)=x_1x_2+x_1x_3+x_2x_3$, $\sigma_3(x_1, x_2, x_3)=x_1x_2x_3$.

n kintamųjų pagrindinių simetrinių polinomų yra n. Juos sutrumpintai žymėsime

$$\sigma_k = \sigma_k(x_1, \ldots, x_n), \quad k = 1, 2, \ldots, n.$$

Polinomas σ_k *yra k-ojo laipsnio forma.*

164 teorema. (Simetrinių polinomų pagrindinė teorema.) *Kiekvieną simetrinį n kintamųjų polinomą* $s(x_1, \ldots, x_n)$ *virš* $\check{Z}$ *galima išreikšti pagrindinių simetrinių polinomų* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *polinomu virš* $\check{Z}$, *t. y.*

$$s(x_1, \ldots, x_n) = F(\sigma_1, \ldots, \sigma_n);$$

čia $F(\sigma_1, \ldots, \sigma_n)$ *— polinomas virš* $\check{Z}$. *Pastaroji išraiška yra vienintelė.*

Įrodymas. Kadangi kiekvienas polinomas yra formų suma, tai simetrinis polinomas taip pat yra formų suma. Be to, formos simetrinės (priešingu atveju polinomas nebūtų simetrinis). Todėl užtenka įrodyti teoremą tuo atveju, kai $s(x_1, \ldots, x_n)$ yra simetrinė forma.

Simetrinę formą $s(x_1, \ldots, x_n)$ išdėstome leksikografiškai ir imame jos vyriausiąjį narį

$$ax_1^{m_1} \ldots x_n^{m_n}.$$

Formos $s(x_1, \ldots, x_n)$ kiekvieno nario laipsnis lygus $m_1+\ldots+m_n$. Įrodysime, kad

$$m_1 \geqslant m_2 \geqslant \ldots \geqslant m_n.$$

Tarkime, kad su kokiu nors k, $m_{k-1} < m_k$. Simetrinėje formoje kartu su nariu

$$ax_1^{m_1} \ldots x_{k-1}^{m_{k-1}} x_k^{m_k} \ldots x_n^{m_n}$$

yra ir narys

$$ax_1^{m_1}\ldots x_{k-1}^{m_k}x_k^{m_k-1}\ldots x_n^{m_n},$$

kuris šiuo atveju vyresnis už pirmąjį. Taigi gauname prieštaravimą vyriausiojo nario parinkimui.

Pažymėkime skirtumus $t_i=m_i-m_{i+1}$, $i=1, \ldots, n-1$, $t_n=m_m$ ir sudaykime polinomą

$$a\sigma_1^{t_1}\sigma_2^{t_2}\ldots\sigma_n^{t_n}.$$

Simetrinių formų sandauga yra simetrinė forma. Kadangi sandaugos vyriausiasis narys yra dauginamųjų vyriausiųjų narių sandauga, tai pastarosios sandaugos vyriausiasis narys yra

$$ax_1^{t_1+\ldots+t_n}x_2^{t_2+\ldots+t_n}\ldots x_{n-1}^{t_{n-1}+t_n}x_n^{t_n}.$$

Bet $t_k+\ldots+t_n=m_k$, todėl *sandaugos*

$$a\sigma_1^{t_1}\ldots\sigma_n^{t_n}$$

vyriausiasis narys yra

$$ax_1^{m_1}\ldots x_n^{m_n},$$

t. y. *sutampa su simetrinės formos* $s(x_1, \ldots, x_n)$ *vyriausiuoju nariu.* Tada skirtumas

$$s(x_1, \ldots, x_n)-a\sigma_1^{t_1}\ldots\sigma_n^{t_n}=s_1(x_1, \ldots, x_n)$$

taip pat simetrinė forma. Formos $s(x_1, \ldots, x_n)$ vyriausiasis narys vyresnis už formos $s_1(x_1, \ldots, x_n)$ kiekvieną (taigi ir vyriausiąjį) narį, nes lygių vyriausiųjų narių skirtumas lygus 0.

Tarkime, kad formos $s_1(x_1, \ldots, x_n)$ vyriausiasis narys yra

$$a_1x_1^{m_1^{(1)}}x_2^{m_2^{(1)}}\ldots x_n^{m_n^{(1)}}.$$

Analogiškai įsitikiname, kad $m_1^{(1)}\geqslant m_2^{(1)}\geqslant\ldots\geqslant m_n^{(1)}$ ir, pažymėję $t_i^{(1)}=m_i^{(1)}-m_{i+1}^{(1)}$, $i=1, \ldots, n-1$, $t_n^{(1)}=m_n^{(1)}$, gauname formą

$$s_2(x_1, \ldots, x_n)=s_1(x_1, \ldots, x_n)-a_1\sigma_1^{t_1^{(1)}}\ldots\sigma_n^{t_n^{(1)}}.$$

Formos $s_1(x_1, \ldots, x_n)$ vyriausiasis narys vyresnis už formos $s_2(x_1, \ldots, x_n)$ kiekvieną narį, taigi ir už vyriausiąjį.

Panašiai samprotaudami toliau, po $j+1$ „žingsnio“ gausime formą

$$s_{j+1}(x_1, \ldots, x_n)=s_j(x_1, \ldots, x_n)-a_j\sigma_1^{t_1^{(j)}}\ldots\sigma_n^{t_n^{(j)}};$$

čia $t_i^{(j)}=m_i^{(j)}-m_{i+1}^{(j)}$, $i=1, \ldots, n-1$, $t_n^{(j)}=m_n^{(j)}$; $m_i^{(j)}$, $i=1, \ldots, n$ – formos $s_j(x_1, \ldots, x_n)$ vyriausiojo nario laipsnio rodikliai.

Kadangi $m_i^{(t)} \geqslant m_{i+1}^{(t)} \geqslant 0$, $i = 1, \ldots, n-1$, $m_1^{(t)} + \ldots + m_n^{(t)} = m_1 + \ldots + m_n$ ir $\{m_1^{(t)}, \ldots, m_n^{(t)}\} \neq \{m_1^{(k)}, \ldots, m_n^{(k)}\}$, kai $t \neq k$, tai rinkinių $m_1^{(t)}, \ldots, m_n^{(t)}$, $t = 1, 2, \ldots, j$, gali būti tik baigtinis skaičius. Todėl

$$s_{j+1}(x_1, \ldots, x_n) = O(x_1, \ldots, x_n).$$

Tada

$$s(x_1, \ldots, x_n) = a\sigma_1^{t_1} \ldots \sigma_n^{t_n} + a_1 \sigma_1^{t_1^{(1)}} \ldots \sigma_n^{t_n^{(1)}} + \ldots + a_j \sigma_1^{t_1^{(j)}} \ldots \sigma_n^{t_n^{(j)}},$$

arba

$$s(x_1, \ldots, x_n) = F(\sigma_1, \ldots, \sigma_n).$$

Taigi pirmoji teoremos dalis įrodyta.

Antroji dalis bus įrodyta įsitikinus, kad lygybė

$$G(\sigma_1, \ldots, \sigma_n) = O(x_1, \ldots, x_n)$$

teisinga tada ir tik tada, kai visi polinomo G koeficientai lygūs nuliui.

Tarkime, kad $G(\sigma_1, \ldots, \sigma_n) = O(x_1, \ldots, x_n)$, o bent vienas jo koeficientas nelygus nuliui. Polinomą $G(\sigma_1, \ldots, \sigma_n)$ užrašome leksikografiškai ir tariame, kad pirmasis nelygus nuliui koeficientas yra $c_{t_1 \ldots t_n} \neq O$. Jį atitinkantis narys yra

$$c_{t_1 \ldots t_n} \sigma_1^{t_1} \ldots \sigma_n^{t_n} = c_{t_1 \ldots t_n} \prod_{k=1}^{n} \Big(\sum_{1 \leqslant j_1 < \ldots < j_k \leqslant n} x_{j_1} \ldots x_{j_k} \Big)^{t_k},$$

t. y. n kintamųjų polinomas. To polinomo vyriausiasis narys yra

$$c_{t_1 \ldots t_n} x_1^{t_1 + \ldots + t_n} x_2^{t_2 + \ldots + t_n} \ldots x_{n-1}^{t_{n-1} + t_n} x_n^{t_n}.$$

Jeigu į polinomą $G(\sigma_1, \ldots, \sigma_n)$ vietoj $\sigma_1, \ldots, \sigma_n$ įrašysime jų išraiškas, tai gausime polinomą $G_1(x_1, \ldots, x_n)$, kurio vyriausiasis narys bus tas pats anksčiau užrašytas narys. Taigi

$$G_1(x_1, \ldots, x_n) = c_{t_1 \ldots t_n} x_1^{t_1 + \ldots + t_n} \ldots x_n^{t_n} + F_1(x_1, \ldots, x_n) = O(x_1, \ldots, x_n).$$

Iš pastarosios lygybės išplaukia, kad $c_{t_1 \ldots t_n} = O$, o tai prieštarauja koeficiento parinkimui. Taigi prielaida neteisinga.

Jeigu $G(\sigma_1, \ldots, \sigma_n) = O(x_1, \ldots, x_n)$, tai visi to polinomo koeficientai lygūs nuliui.

Tarkime, kad kokiu nors būdu gavome išraiškas

$$s(x_1, \ldots, x_n) = F(\sigma_1, \ldots, \sigma_n), \quad s(x_1, \ldots, x_n) = F_1(\sigma_1, \ldots, \sigma_n).$$

Iš pirmosios lygybės panariui atėmę antrąją, gauname

$$G(\sigma_1, \ldots, \sigma_n) = F(\sigma_1, \ldots, \sigma_n) - F_1(\sigma_1, \ldots, \sigma_n) = O(x_1, \ldots, x_n).$$

Iš mūsų samprotavimų išplaukia, kad polinomo $G(\sigma_1, \ldots, \sigma_n)$ visi koeficientai lygūs nuliui. Tai reiškia, kad polinomai F ir F_1 sutampa.

Teoremos įrodymas konstruktyvus. Jį galime pakartoti paėmę bet kokią konkrečią simetrinę formą. Formų $s_1, s_2, \ldots, s_j$ vyriausiųjų narių laipsnių

rodiklius galime rasti išrašę visas tokias galimas skirtingas neneigiamų skaičių $m_1^{(i)}, \ldots, m_n^{(i)}$ kombinacijas, kad būtų $m_1^{(i)} \geqslant m_2^{(i)} \geqslant \ldots \geqslant m_n \geqslant 0$ ir $m_1^{(i)} + m_2^{(i)} + \ldots + m_n^{(i)} = m_1 + m_2 + \ldots + m_n$. Paėmę skirtumus $t_j^{(i)} = m_j^{(i)} - m_{j+1}^{(i)}$, $t_n^{(i)} = m_n^{(i)}$, gausime narius

$$a_i \sigma_1^{t_1^{(i)}} \ldots \sigma_n^{t_n^{(i)}}$$

ir išraišką

$$s(x_1, \ldots, x_n) = a \sigma_1^{t_1} \ldots \sigma_n^{t_n} + \sum_{i=1}^{j} a_i \sigma_1^{t_1^{(i)}} \ldots \sigma_n^{t_n^{(i)}},$$

kurioje bus nežinomi tik koeficientai $a_1, \ldots, a_j$. Tuos koeficientus rasime parinkę $x_1, \ldots, x_n$ konkrečias reikšmes ir sudarę tiesinių lygčių sistemą.

Norėdami praktiškai rasti simetrinio polinomo išraišką pagrindiniais simetriniais polinomais, pirmiausia užrašome simetrinį polinomą simetrinių formų suma. Po to kiekvieną simetrinę formą išreiškiame pagrindiniais simetriniais polinomais ir gautąsias išraiškas sudedame.

Pavyzdys. Polinomą

$$f(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 - 5(x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2)$$

išreikšime pagrindiniais simetriniais polinomais.

Užrašytasis polinomas yra trečiojo laipsnio forma, jos vyriausiasis narys – $x_1^3 x_2^0 x_3^0$. Čia $n=3$, $m_1=3$, $m_2=0$, $m_3=0$. Kadangi nedidėjančių dėmenų suma galimos tik išraiškos $3=3+0+0=2+1+0=1+1+1$, tai

$$f(x_1, x_2, x_3) = \sigma_1^3 + a\sigma_1\sigma_2 + b\sigma_3.$$

Samprotavimus patogu užrašyti lentele:

Galimi vyriausiųjų narių rodikliai	Atitinkami pagrindinių simetrinių polinomų laipsniai	Atitinkamieji nariai
3, 0, 0	3−0, 0−0, 0	σ_1^3
2, 1, 0	2−1, 1−0, 0	$\sigma_1\sigma_2$
1, 1, 1	1−1, 1−1, 1−0	σ_3

Koeficientus a ir b rasime išsprendę lygčių sistemą. Paėmę, pavyzdžiui, $x_1=x_2=x_3=1$, gauname

$$\sigma_1(1, 1, 1) = 1+1+1 = 3, \quad \sigma_2(1, 1, 1) = 1\cdot 1 + 1\cdot 1 + 1\cdot 1 = 3,$$

$$\sigma_3(1, 1, 1) = 1\cdot 1\cdot 1 = 1, \quad f(1, 1, 1) = -27; \quad 27 + 9a + b = -27.$$

Paėmę $x_1=1$, $x_2=1$, $x_3=0$, gauname

$$\sigma_1(1, 1, 0) = 1+1+0 = 2, \quad \sigma_2(1, 1, 0) = 1\cdot 1 + 1\cdot 0 + 1\cdot 0 = 1,$$

$$\sigma_3(1, 1, 0) = 1\cdot 1\cdot 0 = 0, \quad f(1, 1, 0) = -8, \quad \text{t. y.} \quad 8 + 2a = -8.$$

Tos sistemos sprendinys: $a=-8$, $b=18$. Todėl ieškomoji išraiška yra

$$f(x_1, x_2, x_3) = \sigma_1^3 - 8\sigma_1\sigma_2 + 18\sigma_3.$$

Polinomą

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m), \quad n \geqslant 2, \; m \geqslant 2,$$

virš integralumo srities $\check{\mathrm{Z}}$ *vadiname simetriniu pagal kintamųjų sistemas* $x_1, \ldots, x_n$ *ir* $y_1, \ldots, y_m$, *jei su kiekvienu skaičių* $1, 2, \ldots, n$ *kėliniu* $i_1, \ldots, i_n$ *ir su kiekvienu skaičių* $1, 2, \ldots, m$ *kėliniu* $j_1, \ldots, j_m$

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m) = f(x_{i_1}, \ldots, x_{i_n}, y_{j_1}, \ldots, y_{j_m}).$$

Pavyzdys. Polinomas

$$x_1 + x_2 + x_3 - 4y_1y_2 + 7y_1 + 7y_2$$

yra simetrinis pagal dvi kintamųjų sistemas x_1, x_2, x_3 ir y_1, y_2.

Kintamųjų $x_1, \ldots, x_n$ pagrindinius simetrinius polinomus žymėsime $\sigma_1, \ldots, \sigma_n$, o kintamųjų $y_1, \ldots, y_m$ pagrindinius simetrinius polinomus žymėsime $\tau_1, \ldots, \tau_m$.

165 teorema. (Simetrinių polinomų pagrindinės teoremos bendrinys.) *Kiekvieną simetrinį pagal kintamųjų sistemas* $x_1, \ldots, x_n$ *ir* $y_1, \ldots, y_m$ *polinomą* $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$ *virš* $\check{\mathrm{Z}}$ *galima išreikšti pagrindinių simetrinių polinomų* $\sigma_1, \ldots, \sigma_n$ *ir* $\tau_1, \ldots, \tau_m$ *polinomu virš* $\check{\mathrm{Z}}$. *Pastaroji išraiška yra vienintelė.*

Įrodymas. Kadangi

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \check{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m],$$

$$\check{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m] = \check{Z}[x_1, \ldots, x_n][y_1, \ldots, y_m],$$

tai

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m) = f_1(y_1, \ldots, y_m);$$

čia polinomo $f_1(y_1, \ldots, y_m)$ koeficientai yra integralumo srities $\check{\mathrm{Z}}[x_1, \ldots, x_n]$ elementai, t. y. kintamųjų $x_1, \ldots, x_n$ polinomai. Tie *koeficientai yra simetriniai kintamųjų* $x_1, \ldots, x_n$ *polinomai*, nes $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$ simetrinis pagal $x_1, \ldots, x_n$. Be to, $f_1(y_1, \ldots, y_m)$ simetrinis kintamųjų $y_1, \ldots, y_m$ polinomas. Remdamiesi pagrindine teorema apie simetrinius polinomus, gauname

$$f_1(y_1, \ldots, y_m) = f_2(\tau_1, \ldots, \tau_m); \tag{9.1}$$

čia polinomo $f_2(\tau_1, \ldots, \tau_m)$ koeficientai yra kintamųjų $x_1, \ldots, x_n$ simetriniai polinomai virš $\check{\mathrm{Z}}$. Tuos polinomus pagal pagrindinę teoremą apie simetrinius polinomus išreiškę pagrindiniais simetriniais polinomais, gauname

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m) = g(\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m).$$

Pastarosios išraiškos vienatis išplaukia iš (9.1) išraiškos vienaties ir iš polinomo $f_2(\tau_1, \ldots, \tau_m)$ koeficientų išraiškų pagrindiniais simetriniais polinomais $\sigma_1, \ldots, \sigma_n$ vienaties.

Panašiai apibrėžiami ir simetriniai daugiau kaip pagal dvi kintamųjų sistemas polinomai. Lengvai apibendrinama ir 165 teorema.

Uždaviniai

7. Sugalvokite simetrinių polinomų pavyzdžių:
a) dviejų kintamųjų 0, 1, 2, 3, 4 ir 5 laipsnio;
b) trijų kintamųjų 0, 1, 2, 3, 4 ir 5 laipsnio;
c) keturių kintamųjų 0, 1, 2, 3, 4 laipsnio;
d) penkių kintamųjų 0, 1, 3, 5 laipsnio.

8. Užrašykite visus trijų ir keturių kintamųjų pagrindinius simetrinius polinomus.

9. Užrašykite penkių kintamųjų simetrinius polinomus σ_2, σ_3, σ_4 ir šešių kintamųjų simetrinius polinomus σ_2, σ_4.

10. Išreikškite pagrindiniais simetriniais polinomais šiuos polinomus:

a) $x_1^2+x_2^2-2x_1x_2^2-2x_1^2x_2$;
b) $x_1^3+x_2^3+x_1^2+x_2^2-3x_1x_2$;
c) $x_1^3x_2+x_1x_2^3-4x_1x_2+7x_1^2x_2^2-9x_1^2-9x_2^2$;
d) $x_1^2+x_2^2+x_3^2$;
e) $3x_1^2x_2^2x_3^2-x_1x_2x_3^2-x_1x_2^2x_3-x_1^2x_2x_3$;
f) $x_1^2+x_2^2+x_3^2+x_4^2$;
g) $x_1^3+x_2^3+x_3^3$;
h) $(1+2x_1)(1+2x_2)(1+2x_3)$;
i) $(x_1+x_2)(x_1+x_3)(x_2+x_3)$;
j) $x_1^3+x_2^3+x_3^3+x_4^3$.

§83. Vieto formulės. Simetrinių polinomų pagrindinės teoremos išvados

Esame įrodę (žr. 151 teoremą), kad kiekvienas nenulinio laipsnio polinomas $f(x)\in\check{Z}[x]$ turi skaidinio lauką, t. y. minimalų lauką **L**, kuriame polinomas

$$f(x)=\sum_{j=0}^{n} a_j x^j, \quad n\geqslant 1,$$

turi n šaknų. Jas žymėsime $l_1, \ldots, l_n$. Nustatysime polinomo šaknų ir jo koeficientų sąryšius.

166 teorema. *Jeigu*

$$f(x)=\sum_{j=0}^{n} a_j x^j$$

yra n-ojo laipsnio polinomas ($n\geqslant 1$) *ir* $l_1, \ldots, l_n$ *– jo šaknys, tai teisingi sąryšiai*

$$\frac{a_{n-k}}{a_n}=(-1)^k\sigma_k(l_1, \ldots, l_n), \quad k=1, \ldots, n.$$

Tie sąryšiai vadinami *Vieto formulėmis* (Fransua Viete, 1540–1603, prancūzų matematikas).

Įrodymas. Polinomo $f(x)$ ir polinomo

$$f_1(x)=\sum_{j=0}^{n}\frac{a_j}{a_n}x^j$$

šaknys sutampa, nes $a_n f_1(x)=f(x)$.

Iš teoremos apie polinomo išraišką pirminių daugiklių sandauga išplaukia, kad

$$f_1(x)=x^n+\frac{a_{n-1}}{a_n}x^{n-1}+\ldots+\frac{a_1}{a_n}x+\frac{a_0}{a_n}=(x-l_1)(x-l_2)\ldots(x-l_n),$$

kai $\mathbf{L}$ ($\check{Z}\subset L$) yra polinomo $f(x)$ skaidinio laukas. Bet

$$\prod_{j=1}^{n}(x-l_j)=x^n+\sum_{k=1}^{n}(-1)^k\sigma_k(l_1,\ \ldots,\ l_n)x^{n-k},$$

todėl

$$\frac{a_{n-k}}{a_n}=(-1)^k\sigma_k(l_1,\ \ldots,\ l_n),\quad k=1,\ 2,\ \ldots,\ n.$$

Tuo atveju, kai polinomo $f(x)$ vyriausiasis koeficientas $a_n=1$, turime $a_{n-k}=(-1)^k\sigma_k(l_1,\ \ldots,\ l_n)$, $k=1,\ 2,\ \ldots,\ n$.

Kai $n=2$ ir $a_2=1$, gauname

$$a_1=-(l_1+l_2),\quad a_0=l_1l_2,$$

t. y. lygties $x^2+a_1x+a_0=0$ šaknų sandauga lygi laisvajam nariui, o šaknų suma lygi koeficientui prie x su priešingu ženklu.

Naudodamiesi Vieto formulėmis, lengvai gauname pagrindinės teoremos apie simetrinius polinomus išvadą.

167 teorema. *Jeigu* $s(x_1,\ \ldots,\ x_n)$ *yra simetrinis polinomas virš lauko* $\mathbf{L}$, *o* $l_1,\ \ldots,\ l_n$ *yra kurio nors n-ojo laipsnio polinomo* $f(x)$ *virš* $\mathbf{L}$ *šaknys, tai polinomo* $s(x_1,\ \ldots,\ x_n)$ *reikšmė taške* $(l_1,\ \ldots,\ l_n)$ *yra lauko* $\mathbf{L}$ *elementas, t. y.* $s(l_1,\ \ldots,\ l_n)\in L$.

Įrodymas. Kadangi

$$s(x_1,\ \ldots,\ x_n)=F(\sigma_1,\ \ldots,\ \sigma_n)$$

ir F yra polinomas virš $\mathbf{L}$, o

$$\sigma_k(l_1,\ \ldots,\ l_n)=(-1)^k\frac{a_{n-k}}{a_n},\quad k=1,\ \ldots,\ n,$$

tai

$$\sigma_k(l_1,\ \ldots,\ l_n)\in L,\quad k=1,\ 2,\ \ldots,\ n.$$

Bet tada ir

$$s(l_1, \ldots, l_n)=F\big(\sigma_1(l_1, \ldots, l_n), \ldots, \sigma_n(l_1, \ldots, l_n)\big)\in L.$$

Išvada. *Jeigu* $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$ *yra simetrinis pagal kintamųjų* $x_1, \ldots, x_n$ *ir* $y_1, \ldots, y_m$ *sistemas polinomas virš lauko* **L**, *o* $l_1, \ldots, l_n$ *ir* $t_1, \ldots, t_m$ *yra kurių nors n-ojo ir m-ojo laipsnio polinomų virš* **L** *šaknys, tai*

$$f(l_1, \ldots, l_n, t_1, \ldots, t_m)\in L.$$

Išvadą gauname du kartus taikydami teoremą: pirmą kartą (9.1) išraiškos koeficientams, o antrą kartą pačiam polinomui.

Nesunkiai galime gauti išvadą apie polinomo, simetrinio pagal kelias kintamųjų sistemas, reikšmę.

Remdamiesi 164 teorema, gauname dar vieną būdą iracionalumui vardiklyje panaikinti. Imsime racionaliųjų skaičių lauką.

Tarkime, kad reikia gauti išraišką

$$\frac{f(\alpha)}{g(\alpha)}=h(\alpha), \quad g(\alpha)\neq 0;$$

čia α – iracionalusis algebrinis skaičius racionaliųjų skaičių lauko **Q** atžvilgiu, o f, g, h – polinomai virš racionaliųjų skaičių lauko.

Kadangi α – algebrinis skaičius, tai egzistuoja toks pirminis polinomas $p(x)$ su racionaliaisiais koeficientais, kad $p(\alpha)=0$. To polinomo laipsnis yra $n\geqslant 2$, o jo šaknys – $l_1=\alpha, l_2, \ldots, l_n$.

Polinomas $g(x_1)\,g(x_2)\ldots g(x_n)$ yra simetrinis, todėl

$$a=g(\alpha)\,g(l_2)\ldots g(l_n)$$

racionalusis skaičius ir

$$\frac{f(\alpha)}{g(\alpha)}=\frac{f(\alpha)\,g(l_2)\ldots g(l_n)}{g(\alpha)\,g(l_2)\ldots g(l_n)}=\frac{1}{a}\,\big(f(\alpha)\,g(l_2)\ldots g(l_n)\big).$$

Liko rasti daugiklį $g(l_2)\ldots g(l_n)$. Tuo tikslu simetrinį $n-1$ kintamojo polinomą

$$g(x_2)\ldots g(x_n)$$

išreiškiame pagrindiniais simetriniais polinomais

$$g(x_2)\ldots g(x_n)=F(\bar{\sigma}_1, \ldots, \bar{\sigma}_{n-1});$$

čia $\bar{\sigma}_k=\sigma_k(x_2, \ldots, x_n)$, $k=1, 2, \ldots, n-1$.

Į $F(\bar{\sigma}_1, \ldots, \bar{\sigma}_{n-1})$ įrašę $\sigma_k(l_2, \ldots, l_n)$, $k=1, 2, \ldots, n-1$, gausime daugiklį $g(l_2)\ldots g(l_n)$.

Pačius polinomus $\bar{\sigma}_k$ ir jų reikšmes taške $(l_2, \ldots, l_n)$ nesunku rasti iš lygybių

$$\sigma_1=x_1+\bar{\sigma}_1, \quad \sigma_k=x_1\bar{\sigma}_{k-1}+\bar{\sigma}_k, \quad k=2, \ldots, n-1,$$

$$\sigma_n=x_1\bar{\sigma}_{n-1},$$

kurios gaunamos iš išraiškų

$$\bar{\sigma}_k = \sum_{2 \leqslant j_1 < \ldots < j_k \leqslant n} x_{j_1} \ldots x_{j_k}, \quad k = 1, 2, \ldots, n-1,$$

$$\sigma_k = \sum_{1 \leqslant j_1 < \ldots < j_k \leqslant n} x_{j_1} \ldots x_{j_k}, \quad k = 1, 2, \ldots, n.$$

Taigi

$$\bar{\sigma}_1 = \sigma_1 - x_1,$$

$$\bar{\sigma}_2 = \sigma_2 - x_1 \bar{\sigma}_2 \text{ ir t.t.}$$

Pavyzdys. Panaikinsime iracionalumą vardiklyje:

$$\frac{3}{2 - \sqrt[4]{3} + \sqrt{3}}.$$

Pastebime, kad $(\sqrt[4]{3})^2 = \sqrt{3}$. Pažymėję $\alpha = \sqrt[4]{3}$, gauname

$$g(\alpha) = \alpha^2 - \alpha + 2,$$

$$g(x) = x^2 - x + 2.$$

Be to, $\alpha = \sqrt[4]{3}$ yra polinomo

$$p(x) = x^4 - 3$$

šaknis. Pažymėję to polinomo šaknis $l_1 = \alpha$, l_2, l_3, l_4, sudarome simetrinį polinomą

$$G = (x_2^2 - x_2 + 2)(x_3^2 - x_3 + 2)(x_4^2 - x_4 + 2),$$

išreiškiame jį pagrindiniais simetriniais polinomais

$$\bar{\sigma}_1 = \sigma_1(x_2, x_3, x_4), \quad \bar{\sigma}_2 = \sigma_2(x_2, x_3, x_4), \quad \bar{\sigma}_3 = \bar{\sigma}_3(x_2, x_3, x_4)$$

ir gauname

$$G = \bar{\sigma}_3^2 - \bar{\sigma}_3\sigma_2 - 3\bar{\sigma}_3\bar{\sigma}_1 + 5\bar{\sigma}_3 + 4\bar{\sigma}_2^2 - 2\bar{\sigma}_2\bar{\sigma}_1 - 6\bar{\sigma}_2 + 4\bar{\sigma}_1^2 + 4\bar{\sigma}_1 + 8.$$

Dabar apskaičiuojame $\bar{\sigma}_1$, $\bar{\sigma}_2$ ir $\bar{\sigma}_3$ reikšmes taške (l_2, l_3, l_4).

Kadangi α, l_2, l_3, l_4 yra polinomo $x^4 - 3$ šaknys, tai iš Vieto formulių išplaukia, kad

$$\alpha + \bar{\sigma}_1 = 0, \qquad \bar{\sigma}_1 = -\alpha = -\sqrt[4]{3},$$

$$\alpha\bar{\sigma}_1 + \bar{\sigma}_2 = 0, \qquad \bar{\sigma}_2 = -\alpha\bar{\sigma}_1 = \alpha_2 = \sqrt{3},$$

$$\alpha\bar{\sigma}_2 + \bar{\sigma}_3 = 0, \qquad \bar{\sigma}_3 = -\alpha\bar{\sigma}_2 = -\sqrt[4]{27}.$$

$$\alpha\bar{\sigma}_3 = -3,$$

Įrašę tas reikšmes į G išraišką ir atlikę veiksmus, gauname

$$G(l_2, l_3, l_4) = -3\sqrt[4]{27} + 7\sqrt[4]{3} + \sqrt{3} + 5$$

ir

$$(\sqrt[4]{9} - \sqrt[4]{3} + 2)\, G(l_2, l_3, l_4) = 22.$$

Taigi

$$\frac{3}{2-\sqrt[4]{3}+\sqrt{3}}=\frac{3}{22}(5+7\sqrt[4]{3}+\sqrt{3}-3\sqrt[4]{27}).$$

Uždaviniai

11. Apskaičiuokite pagrindinių simetrinių polinomų $\sigma_k(x_1, \ldots, x_n)$, $k=1, \ldots, n$, reikšmes taške $(l_1, \ldots, l_n)$, kai $l_1, \ldots, l_n$ – šitokio polinomo šaknys:

a) $x^5-6x^3+4x-27$;
b) $3x^4-7x^3+x^2+x-6$;
c) $13x^7-5x^6-4x^2+39x+26$;
d) $x^9-2x^7+3x^5-3x^2$;
e) $3x^8-2x^7+4x^4-6x+13$.

12. Apskaičiuokite simetrinio polinomo $s(x_1, \ldots, x_n)$ reikšmę taške $(l_1, \ldots, l_n)$, kai $l_1 \ldots, l_n$ yra polinomo $f(x)$ šaknys:

a) $s(x_1, x_2, x_3)=x_1^4+x_2^4+x_3^4$, $f(x)=2x^3-6x^2-3x+5$;
b) $s(x_1, x_2, x_3)=(x_1+x_2-x_3)(x_1-x_2+x_3)(-x_1+x_2+x_3)$, $f(x)=x^3+5x^2-x+2$;
c) $s(x_1, x_2, x_3, x_4)=(x_1+1)(x_2+1)(x_3+1)(x_4+1)$, $f(x)=2x^4-3x^3+5x-6$.

13. Remdamiesi simetrinių polinomų išraiška pagrindiniais simetriniais polinomais, panaikinkite iracionalumą vardiklyje:

a) $\frac{1}{2-3\sqrt[3]{2}+\sqrt[3]{4}}$; b) $\frac{1}{1-\sqrt[3]{5}+\sqrt[3]{25}}$; c) $\frac{1}{2+\sqrt[4]{2}}$; d) $\frac{1}{\sqrt[5]{3}-1}$.

§84. Rezultantas ir jo taikymai

Tarkime, kad

$$g(x)=\sum_{j=n}^{0} b_j x^j, \quad h(x)=\sum_{j=m}^{0} c_j x^j$$

yra du polinomai virš nulinės charakteristikos lauko **L**, kurių laipsniai atitinkamai lygūs n ir m, t. y. $b_n \neq 0$ ir $c_m \neq 0$.

Polinomų $g(x)$ ir $h(x)$ rezultantu $R(g, h)$ vadinamas $m+n$-osios eilės determinantas, sudarytas iš polinomų $g(x)$ ir $h(x)$ koeficientų:

$$R(g, h)=\begin{vmatrix} b_n & b_{n-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\ 0 & b_n & \ldots & b_2 & b_1 & b_0 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & b_n & b_{n-1} & b_{n-2} & \ldots & b_0 \\ c_m & c_{m-1} & \ldots & c_1 & c_0 & 0 & \ldots & 0 \\ 0 & c_m & \ldots & c_2 & c_1 & c_0 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & c_m & c_{m-1} & & \ldots & c_0 \end{vmatrix}$$

To determinanto pirmąsias m eilučių gauname šitaip: polinomo $g(x)$ koeficientus $b_n, b_{n-1}, \ldots, b_1, b_0$ surašome 1-oje eilutėje ir kiekvienoje tolesnėje eilutėje rašome juos ta pačia tvarka pastumdami į dešinę per vieną vietą. Ki-

tose tų eilučių vietose rašome nulį. n paskutinių eilučių gauname tokiu pat būdu įrašydami polinomo $h(x)$ koeficientus $c_m, c_{m-1}, \ldots, c_2, c_1, c_0$.

Iš apibrėžimo išplaukia, kad

$$R(h, g)=\begin{vmatrix} c_m & c_{m-1} & \ldots & c_0 & 0 & \ldots & 0 \\ 0 & c_m & \ldots & c_1 & c_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & c_m & c_{m-1} & \ldots & c_0 \\ b_n & b_{n-1} & \ldots & b_1 & b_0 & \ldots & 0 \\ 0 & b_n & \ldots & b_2 & b_1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_n & b_{n-1} & \ldots & 0 \end{vmatrix}.$$

Pastarąjį determinantą galime gauti iš pirmojo perkėlę paskutines n eilučių į pirmąsias vietas. Kiekvieną eilutę reikia sukeisti vietomis su m eilučių. Iš atitinkamos determinanto savybės išplaukia lygybė

$$R(g, h)=(-1)^{mn} R(h, g).$$

Pavyzdys. Jeigu

$$g(x)=3x^4-6x^3+5x^2-7x+15,$$

$$h(x)=6x^2-4x-3,$$

tai

$$R(g, h)=\begin{vmatrix} 3 & -6 & 5 & -7 & 15 & 0 \\ 0 & 3 & 6 & 5 & -7 & 15 \\ 6 & -4 & -3 & 0 & 0 & 0 \\ 0 & 6 & -4 & -3 & 0 & 0 \\ 0 & 0 & 6 & 4 & -3 & 0 \\ 0 & 0 & 0 & 6 & 4 & -3 \end{vmatrix}=687\,169.$$

168 teorema. *Jeigu $g(x)$ ir $h(x)$ yra atitinkamai n-ojo $(n \geqslant 1)$ ir m-ojo $(m \geqslant 1)$ laipsnių polinomai virš nulinės charakteristikos lauko, tai $R(g, h)=O$ tada ir tik tada, kai tie polinomai turi bendrą netrivialųjį daliklį.*

Įrodymas. Polinomai $g(x)$ ir $h(x)$ turi bendrą nenulinio laipsnio daliklį tada ir tik tada, kai egzistuoja tokie nelygūs nuliui polinomai $g_1(x)$ ir $h_1(x)$, kurių laipsniai mažesni atitinkamai už polinomų $g(x)$ ir $h(x)$ laipsnius, su kuriais teisinga lygybė

$$g(x) h_1(x)+h(x) g_1(x)=O(x) \tag{9.2}$$

(žr. § 72, 143 teoremą).

Kadangi

$$g(x)=\sum_{j=n}^{0} b_j x^j, \quad h(x)=\sum_{j=m}^{0} c_j x^j,$$

tai pažymėję polinomų $g_1(x)$ ir $h_1(x)$ koeficientus u_i $(i=n-1, \ldots, 1, 0)$, v_i $(i=m-1, \ldots, 0)$, t. y.

$$g_1(x)=\sum_{i=n-1}^{0} u_i x^i, \quad h_1(x)=\sum_{i=m-1}^{0} v_i x^i,$$

iš (9.2) lygybės gauname lygybę

$$\sum_{k=m+n-1}^{0}\Big(\sum_{j+i=k} b_j v_i+\sum_{l+r=k} c_l u_r\Big) x^k=O(x),$$

o pastaroji ekvivalenti lygybių sistemai

$$\sum_{j+i=k} b_j v_i+\sum_{l+r=k} c_l u_r=0, \quad k=m+n-1, \ldots, 1, 0. \tag{R}$$

Kai polinomai $g_1(x)$ ir $h_1(x)$ nežinomi, (R) yra $m+n$ homogeninių tiesinių lygčių sistema su kintamaisiais $v_{m-1}, \ldots, v_0, u_{n-1}, \ldots, u_0$.

Iš (9.2) lygybės išplaukia, kad homogeninių lygčių sistema (R) turi nenulinį sprendinį. Taip yra tada ir tik tada, kai tos sistemos determinantas Δ lygus nuliui.

Sistemos (R) determinantas yra

$$\Delta=\begin{vmatrix} b_n & & O & c_m & & O \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & \ddots & \vdots & & \ddots \\ b_0 & & b_n & c_0 & & c_m \\ & \ddots & \vdots & & \ddots & \vdots \\ & & \vdots & & & \vdots \\ O & & b_0 & O & & c_0 \end{vmatrix},$$

t. y. $R(g, h)=\Delta$.

Kadangi $\Delta=O$ tada ir tik tada, kai teisinga (9.2) lygybė, t. y. kai polinomai $g(x)$ ir $h(x)$ turi nenulinio laipsnio bendrąjį daliklį, tai iš lygybės $R(g, h)=\Delta$ išplaukia teoremos tvirtinimas.

Polinomo $g(x)$ šaknis pažymėję $l_1, \ldots, l_n$, o polinomo $h(x)$ šaknis — $t_1, \ldots, t_m$, gausime išraiškas

$$g(x)=b_n(x-l_1)\ldots(x-l_n),$$
$$h(x)=c_m(x-t_1)\ldots(x-t_m).$$

169 teorema.

$$R(g, h)=b_n^m c_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(l_i-t_j), \tag{9.3}$$

$$R(g, h)=b_n^m \prod_{i=1}^{n} h(l_i), \tag{9.4}$$

$$R(g, h)=(-1)^{mn} c_m^n \prod_{j=1}^{m} g(t_j). \tag{9.5}$$

Įrodymas. Tarkime, kad (9.3) išraiška teisinga. Kadangi

$$h(l_i)=c_m\prod_{j=1}^{m}(l_i-t_j),$$

tai

$$\prod_{i=1}^{n}h(l_i)=c_m^n\prod_{i=1}^{n}\prod_{j=1}^{m}(l_i-t_j).$$

Pastarąją lygybę padauginę iš b_n^m, gauname (9.4) išraišką.

Jeigu (9.3) išraiška teisinga, tai teisinga ir išraiška

$$R(g,\ h)=(-1)^{mn}b_n^m c_n^m\prod_{i=1}^{n}\prod_{j=1}^{m}(t_j-l_i),$$

kuri gaunama iš (9.3) išraiškos, pasinaudojus lygybėmis

$$l_i-t_j=-(t_j-l_i).$$

Pastebėję, kad

$$g(t_j)=b_n\prod_{i=1}^{n}(t_j-l_i),$$

lengvai gauname (9.5) išraišką.

Taigi užtenka įrodyti tik (9.3) rezultanto išraišką.

n kintamųjų pagrindinių simetrinių polinomų reikšmes taške $(l_1, \ldots, l_n)$ žymėsime s_k, t. y.

$$s_k=\sigma_k(l_1,\ \ldots,\ l_n),\quad k=1,\ \ldots,\ n,$$

m kintamųjų pagrindinių simetrinių polinomų reikšmes taške $(t_1, \ldots, t_m$ žymėsime τ_k, t. y.

$$\tau_k=\sigma_k(t_1,\ \ldots,\ t_m),\quad k=1,\ 2,\ \ldots,\ m.$$

Pasinaudoję Vieto formulėmis

$$b_k=(-1)^{n-k}s_{n-k}b_n,\quad k=n,\ \ldots,\ 1,$$
$$c_k=(-1)^{m-k}\tau_{m-k}c_m,\quad k=m,\ \ldots,\ 1,$$

ir pastaraisias koeficientų b_k ir c_k išraiškas įrašę į rezultanto $R\ (g,\ h)$ išraišką determinantu, gauname determinantą, kurio kiekviena iš pirmųjų m eilučių turi daugiklį b_n, o kiekviena iš paskutinių n eilučių – daugiklį c_m. Taigi

$$R(g,\ h)=b_n^m c_m^n R_1(g,\ h);$$

čia $R_1\ (g, h)$ – polinomas iš $L[s_1, \ldots, s_n, \tau_1, \ldots, \tau_m]$, t. y. polinomas iš $L\ [l_1, \ldots, l_n, t_1, \ldots, t_m]$, nes $s_1, \ldots, s_n$ yra kintamųjų $l_1, \ldots, l_n$ polinomai, o $\tau_1, \ldots, \tau_m$ – kintamųjų $t_1, \ldots, t_m$ polinomai.

Jeigu lygybėje

$$g(x)=b_n\prod_{i=1}^{n}(x-l_i)$$

vietoj bet kurio l_k įrašysime t_r, tai gausime išraiškas

$$g_r(x)=b_n(x-t_r)\prod_{\substack{i=1\\ i\neq r}}^{n}(x-l_i),$$

$$h(x)=c_m\prod_{j=1}^{m}(x-t_j),$$

iš kurių aiškiai matyti, kad polinomai $g_r(x)$ ir $h(x)$ turi bendrąjį daliklį $(x-t_r)$. Taigi, kai $l_k=t_r$, tada $R(g, h)=O$, t. y. ir $R_1(g, h)=O$.

Pastaroji lygybė reiškia, kad $R_1(g, h)$ dalijasi iš l_k-t_r. Kadangi k ($k=1, \ldots, n$) ir r ($r=1, 2, \ldots, m$) galime imti bet kokius, *tai* $R_1(g, h)$ *dalijasi iš visų galimų skirtumų* l_i-t_j, t. y. dalijasi iš

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(l_i-t_j).$$

Taigi

$$R(g, h)=\left(b_n^m c_m^n\prod_{i=1}^{n}\prod_{j=1}^{m}(l_i-l_j)\right)R_2(g, h). \tag{9.6}$$

Pirmiausia įrodysime, kad $R_1(g, h)$ yra mn-ojo laipsnio forma kintamųjų $l_1, \ldots, l_n, t_1, \ldots, t_m$ atžvilgiu.

Kadangi $R_1(g, h)=|(c_{ij})|$ yra $m+n$-osios eilės determinantas, kurio elementai, neatsižvelgiant į ženklą, išreiškiami šitaip:

$$\bar{c}_{ij}=\begin{cases}1, & i=j,\ 1\leqslant j\leqslant m,\\ s_{j-i}, & i\leqslant j\leqslant n+i,\ 1\leqslant i\leqslant m,\\ 1, & i=m+j,\ 1\leqslant j\leqslant n,\\ \tau_{m-i+j}, & m+1\leqslant i\leqslant m+n,\ i-m\leqslant j\leqslant i,\\ 0 & \text{kitais atvejais,}\end{cases}$$

tai to determinanto bendrasis narys yra

$$c_{1j_1}c_{2j_2}\ldots c_{m+n\,j_{m+n}};$$

čia $j_1, j_2, \ldots, j_{m+n}$ – skaičių 1, 2, ..., $m+n$ kėlinys. Vietoj c_{ij} įrašę $\bar{c}_{ij}$, gausime nelygaus nuliui nario, kuris yra simetrinių polinomų s_k ir τ_l sandauga, indeksų sumą ($s_0=1$, $\tau_0=1$)

$$\sum_{i=1}^{m}(j_i-i)+\sum_{i=m+1}^{m+n}(m-i+j_i)=mn+\sum_{i=1}^{m+n}(j_i-i)=mn,$$

nes paskutinė suma lygi nuliui.

Tai reiškia, kad determinanto $R_1(g, h)$ kiekvienas narys (neatsižvelgiant į ženklą) yra šitokio pavidalo:

$$s_{k_1}\ldots s_{k_n}\tau_{i_1}\ldots\tau_{i_m},$$

$$k_1+\ldots+k_n+i_1+\ldots+i_m=mn.$$

Iš čia išplaukia, kad polinomo $R_1(g, h)$ kiekvieno nario išraiška yra

$$l_1^{r_1}\ldots l_n^{r_n}t_1^{u_1}\ldots t_m^{u_m}$$

ir $r_1+\ldots+r_n+u_1+\ldots+u_m=mn$. Taigi polinomas $R_1(g, h)$ yra mn-ojo laipsnio forma.

Kadangi

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(l_i-t_j)$$

taip pat yra mn-ojo laipsnio forma, o dauginant polinomus, jų laipsniai sudedami, tai iš išraiškos

$$R_1(g, h)=\left(\prod_{i=1}^{n}\prod_{j=1}^{m}(l_i-t_j)\right)R_2(g, h)$$

išplaukia, kad $R_2(g, h)$ yra nulinio laipsnio polinomas, t. y.

$$R_2(g, h)=a\in L.$$

Paėmę $l_1=\ldots=l_n=O$, gauname $b_0=\ldots=b_{n-1}=O$ ir

$$R(g, h)=b_n^m c_0^n=ab_n^m c_m^n\left(\prod_{j=1}^{m}(-t_j)\right)^n.$$

Tačiau

$$\prod_{j=1}^{m}(-t_j)=(-1)^m\tau_m=\frac{c_0}{c_m}.$$

Todėl

$$b_n^m c_0^n=ab_n^m c_m^n\left(\frac{c_0}{c_m}\right)^n,\quad c_0\neq 0,\ \text{ir}\ a=1.$$

Kadangi $R_2(g, h)=1$, tai (9.3) rezultanto išraiška išplaukia iš (9.6) lygybės.

Išvada. *Iš* (9.3)–(9.5) *išraiškų išplaukia, kad* $R(g, h)=O$ *tada ir tik tada, kai polinomai* $g(x)$ *ir* $h(x)$ *turi bent vieną bendrą šaknį.*

Remdamiesi įrodytąja teorema, polinomo

$$f(x)=\sum_{j=n}^{0} a_j x^j$$

ir jo išvestinės

$$f'(x)=\sum_{j=n}^{1} j a_j x^{j-1}$$

rezultantą išreiškiame šitaip:

$$R(f, f')=a_n^{2n-1} n^n \prod_{i=1}^{n} \prod_{j=1}^{n-1} (l_i-t_j)=a_n^{n-1} \prod_{i=1}^{n} f'(l_i)=$$

$$=(-1)^{n(n-1)}(na_n)^n \prod_{j=1}^{n-1} f(t_j);$$

čia $l_1, \ldots, l_n$ – polinomo $f(x)$ šaknys, $t_1, \ldots, t_{n-1}$ – jo išvestinės $f'(x)$ šaknys.

Prisiminę, kad

$$f(x)=a_n \prod_{i=1}^{n} (x-l_i)$$

ir

$$f'(x)=a_n \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (x-l_j),$$

gauname

$$f'(l_i)=a_n \prod_{\substack{j=1 \\ j\neq i}}^{n} (l_i-l_j).$$

Pastarąsias išraiškas įrašę į lygybę

$$R(f, f')=a_n^{n-1} \prod_{i=1}^{n} f'(l_i),$$

gauname išraišką

$$R(f, f')=a_n^{2n-1} \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (l_i-l_j)=(-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} \prod_{1\leqslant i<j\leqslant n} (l_i-l_j)^2,$$

iš kurios išplaukia lygybė

$$a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (l_i - l_j)^2 = (-1)^{\frac{n(n-1)}{2}} R(f, f') a_n^{-1}.$$

Polinomo

$$f(x) = \sum_{j=n}^{0} a_j x^j$$

diskriminantu vadinamas reiškinys

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{-1} R(f, f').$$

Iš įrodytųjų lygybių gauname

$$D(f) = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (l_i - l_j)^2;$$

čia $l_1, \ldots, l_n$ – polinomo $f(x)$ šaknys. Iš pastarosios lygybės išplaukia šitoks teiginys: *polinomas $f(x)$ turi kartotinių šaknų tada ir tik tada, kai jo diskriminantas lygus nuliui.*

Atkreipsime dėmesį, kad tuo atveju, kai $a_n = 1$,

$$D(f) = \prod_{1 \leqslant i < j \leqslant n} (l_i - l_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leqslant i \neq j \leqslant n} (l_i - l_j) = (-1)^{\frac{n(n-1)}{2}} R(f, f') =$$

$$= (-1)^{\frac{n(n-1)}{2}} \begin{vmatrix} 1 & a_{n-1} & \ldots & a_2 & a_1 & a_0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & a_3 & a_2 & a_1 & a_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & a_{n-1} & a_{n-2} & \cdot & \ldots & a_0 \\ n & (n-1)a_{n-1} & \ldots & 2a_2 & a_1 & 0 & 0 & \ldots & 0 \\ 0 & n & \ldots & 3a_3 & 2a_2 & a_1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & n & (n-1)a_{n-1} & \cdot & \ldots & a_1 \end{vmatrix}.$$

Iš mokyklinio matematikos kurso žinome, kad kvadratinio trinario $f(x) = x^2 + px + q$ diskriminantu vadinamas reiškinys $p^2 - 4q$. Kadangi $p = -(l_1 + l_2)$, o $q = l_1 l_2$, l_1, l_2 – trinario šaknys, tai $p^2 - 4q = (l_1 + l_2)^2 - 4l_1 l_2 = (l_1 - l_2)^2$. Pagal bendrą diskriminanto apibrėžimą

$$D(f) = (l_1 - l_2)^2.$$

Taigi tuo atveju abi šios sąvokos sutampa.

Nustatėme, kad naudodamiesi rezultantu bei 169 teoremos išvada, galime išaiškinti, ar du polinomai turi bendrų šaknų. Skaičiuodami polinomo $f(x)$ ir jo išvestinės rezultantą $R(f, f')$, galime nustatyti, ar polinomas turi kartotinių šaknų.

Naudodamiesi rezultantu, dviejų lygčių su dviem kintamaisiais sistemos sprendimą galime pakeisti vienos lygties su vienu kintamuoju sprendimu.

Imkime du dviejų kintamųjų polinomus $f(x, y)$ ir $g(x, y)$. Užrašę tuos polinomus virš $\mathbf{L}[x]$, gauname

$$f(x, y)=\sum_{j=n}^{0} a_j(x)\, y^j,$$

$$g(x, y)=\sum_{j=m}^{0} b_j(x)\, y^j.$$

Jeigu lygtys

$$f(x, y)=O,$$

$$g(x, y)=O$$

turi bendrą sprendinį (l, t), tai reiškia, kad polinomų

$$f(l, y)=\sum_{j=n}^{0} a_j(l)\, y^j,$$

$$g(l, y)=\sum_{j=m}^{0} b_j(l)\, y^j$$

rezultantas lygus nuliui, t. y.

$$R_l(f, g)=O.$$

Jeigu $R_l(f, g)=O$ su kuriuo nors l, tai polinomai $f(l, y)$ ir $g(l, y)$ turi bendrą šaknį t. Tuomet (l, t) yra sistemos

$$f(x, y)=O,$$

$$g(x, y)=O$$

sprendinys, nes $f(l, t)=O$, $g(l, t)=O$.

Iš viso to išplaukia, kad, *norint išspręsti sistemą*

$$f(x, y)=O,$$

$$g(x, y)=O,$$

reikia sudaryti rezultantą $R_x(f, g)$ *ir spręsti lygtį*

$$R_x(f, g)=O.$$

Radus tos lygties šaknis $l_1, \ldots, l_N$, *reikia rasti polinomų* $f(l_i, y)$ *ir* $g(l_i, y)$ *bendrąsias šaknis* $t_{i_1}, \ldots, t_{i_{r_i}}$. *Gautosios poros* (l_i, t_{i_j}) $(i=1, 2, \ldots, N;\ j=1, \ldots, r_i)$ *ir bus sistemos sprendiniai.*

Spręsdami lygčių sistemą nurodytuoju būdu, eliminuojame nežinomąjį y, t. y. gauname lygtį

$$R_x(f, g)=O.$$

Užrašę polinomus šitaip:

$$f(x,\ y)=\sum_{j=n_1}^{0} c_j(y)\,x^j,$$

$$g(x,\ y)=\sum_{j=m_1}^{0} d_j(y)\,x^j,$$

gauname lygtį

$$R_y(f,\ g)=O,$$

kurioje nėra x. Radę tos lygties sprendinius $t_1, \ldots, t_m$, sistemos sprendinius rasime nustatę polinomų $f(x, t_j)$ ir $g(x, t_j)$ bendrąsias šaknis $l_{j_1}, \ldots, l_{j_n}$ ir paėmę poras (l_{j_i}, t_j) $(j=1, 2, \ldots, m;\ i=1, \ldots, n_j)$.

Pavyzdys. Išspręsime lygčių sistemą

$$y^2-7xy+4x^2+13x-2y-3=0,$$

$$y^2-14xy+9x^2+28x-4y-5=0.$$

Naudodamiesi rezultantu, iš lygčių sistemos eliminuojame y. Sistemą užrašome šitaip:

$$y^2+y(-7x-2)+(4x^2+13x-3)=0,$$

$$y^2+y(-14x-4)+(9x^2+28x-5)=0.$$

Sudarome ir apskaičiuojame rezultantą $R_x(f, g)$:

$$R_x(f,\ g)=\begin{vmatrix} 1 & -7x-2 & 4x^2+13x-3 & 0 \\ 0 & 1 & -7x-2 & 4x^2+13x-3 \\ 1 & -14x-4 & 9x^2+28x-5 & 0 \\ 0 & 1 & -14x-4 & 9x^2+28x-5 \end{vmatrix}=-24x(x-1)(x-2)(x+2).$$

Prilyginę rezultantą nuliui, gauname lygtį

$$x(x-1)(x-2)(x+2)=0,$$

kurios šaknys yra $l_1=0$, $l_2=1$, $l_3=2$, $l_4=-2$.

Tas x reikšmes įrašome į sistemos lygtis ir randame gautųjų lygčių bendrąsias šaknis (gautųjų sistemų sprendinius).

1) $l_1=0$;

$$y^2-2y-3=0,$$

$$y^2-4y-5=0.$$

Sistemos sprendinys yra $t_1=-1$. Todėl pradinės sistemos vienas sprendinys yra $(0, -1)$.

2) $l_2=1$;

$$y^2-9y+14=0,$$

$$y^2-18y+32=0.$$

Gauname sistemos sprendinį $t_2=2$. Taigi pradinės sistemos sprendinys yra $(1, 2)$.

3) $l_3=2$;

$$y^2-16y+39=0,$$

$$y^2-32y+87=0.$$

Tos sistemos sprendinys yra $t_3=3$, o pradinės sistemos sprendinys — (2, 3).

4) $l_4=-2$;

$$y^2+12y-13=0,$$

$$y^2+24y-25=0.$$

Randame sistemos sprendinį $t_4=1$, todėl pradinės sistemos sprendinys yra $(-2, 1)$. Taigi sistemos sprendiniai yra

$$(0, -1),\ (1, 2),\ (2, 3),\ (-2, 1).$$

Uždaviniai

14. Apskaičiuokite polinomo diskriminantą ir kartu nustatykite, ar polinomas turi kartotinių šaknų:

a) $3x^3+2x^2-x+5$;
c) x^3+x^2-4x+3;
b) $2x^4-3x^3-6x^2-2x-1$;
d) $2x^4-6x+1$.

15. Apskaičiuokite šių polinomų rezultantus:

a) $3x^2+x-2$, x^2-2x-2;
b) x^2-2x+4, x^3+2x^2+2x-2;
c) x^3+x^2-x-1, x^3-3x+6.

16. Naudodamiesi rezultantu, išspręskite lygčių sistemas:

a) $3x^2+4xy-2y^2+6x+24y-24=0$, $8x^2+20xy+11y^2-12x-6y-8=0$;
b) $4x^2-7xy+y^2+28x-11y+24=0$, $9x^2-14xy+y^2+60x-20y+51=0$;
c) $x^3-xy^2+5x^2-y^2+7x+3=0$,
$x^4-6x^2y^2+y^4+6x^3-12xy^2+13x^2-6y^2+14x+6=0$.

Polinomai virš skaičių laukų

§85. Kompleksinių skaičių lauko algebrinis uždarumas

Šiame skyriuje nagrinėsime polinomus, kurių koeficientai yra kompleksiniai (atskiru atveju realieji arba racionalieji) skaičiai, t. y. polinomus iš $\mathbf{K}[x]$ (iš $\mathbf{R}[x]$ arba $\mathbf{Q}[x]$).

Esame įrodę (žr. § 76, 151 teoremą), kad egzistuoja toks kiekvieno lauko $\mathbf{L}$ plėtinys $\mathbf{L}'$ ($L \subset L'$), kuriame kiekvienas n-ojo laipsnio polinomas ($n \geqslant 1$) iš $\mathbf{L}[x]$ turi n šaknų. Šio paragrafo tikslas – išaiškinti, kokiame lauke kiekvienas nenulinio laipsnio polinomas su kompleksiniais (arba realiaisiais) koeficientais turi šaknį. Įrodysime pagrindinę klasikinės algebros teoremą.

Kiekvienas nenulinio laipsnio polinomas su kompleksiniais (taigi ir su realiaisiais) koeficientais turi šaknį kompleksinių skaičių lauke $\mathbf{K}$.

Iš tos teoremos išplaukia, kad *kompleksinių skaičių laukas* $\mathbf{K}$ *yra algebriškai uždaras*. Nesunku patikrinti, kad *laukai* $\mathbf{Q}$ *ir* $\mathbf{R}$ *nėra algebriškai uždari*. Pakanka imti polinomą x^2+1, kuris neturi realiųjų šaknų.

Suformuluotosios teoremos įrodymą pirmasis paskelbė K. F. Gausas 1799 metais. Vėliau jis kelis kartus tobulino tą įrodymą.

Šiuo metu žinoma apie 50 skirtingų tos teoremos įrodymų. Dauguma jų paremti kompleksinio kintamojo funkcijų teorija.

Įrodysime minėtąją teoremą algebriniu būdu, naudodamiesi tik vienu matematinės analizės faktu – Bolcano teorema. Toks įrodymas nėra paprastas ir reikalauja nemažo paruošiamojo darbo (kaip ir kiekvienas kitas tos teoremos įrodymas).

Bendroji teoremos įrodymo schema yra šitokia:

1) įrodoma, kad kiekvienas nenulinio laipsnio polinomas su realiaisiais koeficientais turi šaknį kompleksinių skaičių lauke $\mathbf{K}$ (1–2 lemos);

2) remiantis pirmąja dalimi, įrodoma, kad kiekvienas nenulinio laipsnio polinomas su kompleksiniais koeficientais turi šaknį kompleksinių skaičių lauke $\mathbf{K}$ (3–4 lemos, pagrindinė teorema).

1 lema. *Kiekvienas nelyginio laipsnio polinomas su realiaisiais koeficientais* ($f(x) \in \mathbf{R}[x]$) *turi realią šaknį.*

Įrodymas. Tarkime, kad $n=2m+1$ ir

$$f(x)=\sum_{j=2m+1}^{0} a_j x^j.$$

Nemažindami bendrumo, galime laikyti $a_{2m+1}=1$. Pertvarkę tos lygybės dešiniąją pusę, kai $x\neq 0$, gauname

$$f(x)=x^{2m+1}\left(1+\frac{a_{n-1}}{x}+\ldots+\frac{a_0}{x^n}\right)=x^{2m+1}\left(1+g\left(\frac{1}{x}\right)\right).$$

Paėmę $|x|>n\max\limits_{0\leqslant j\leqslant n-1}\{|a_j|\}=a$ ir $|x|\geqslant 1$, turime

$$\left|g\left(\frac{1}{x}\right)\right|\leqslant\frac{1}{|x|}\left(|a_{n-1}|+\frac{|a_{n-2}|}{|x|}+\ldots+\frac{|a_0|}{|x^{n-1}|}\right)\leqslant$$

$$\leqslant\frac{1}{|x|}\sum_{j=n-1}^{0}|a_j|\leqslant\frac{na}{|x|}<1.$$

Taigi, kai $|x|\geqslant b=\max\{a, 1\}$, teisinga nelygybė

$$1+g\left(\frac{1}{x}\right)\geqslant 1-\left|g\left(\frac{1}{x}\right)\right|>0.$$

Remdamiesi ta nelygybe, gauname

$$f(b)=b^{2m+1}\left(1+g\left(\frac{1}{b}\right)\right)>0$$

ir

$$f(-b)=(-b)^{2m+1}\left(1+g\left(\frac{1}{-b}\right)\right)=-b^{2m+1}\left(1+g\left(\frac{1}{-b}\right)\right)<0.$$

Bolcano teorema teigia: *uždarajame intervale* $[-b, b]$ *tolydžioji funkcija* $f(x)$, *kuri intervalo galuose įgyja skirtingų ženklų reikšmes, bent vieną to intervalo tašką* x_0 *atvaizduoja į nulį, t. y.* $(\exists x_0\in[-b, b])\ f(x_0)=0$.

Polinomo $f(x)$ su realiaisiais koeficientais apibrėžta funkcija aibėje **R** yra tolydi. Todėl jai galima taikyti Bolcano teoremą.

Taigi 1 lema įrodyta.

2 lema. *Kiekvienas nenulinio laipsnio su realiaisiais koeficientais polinomas turi šaknį kompleksinių skaičių lauke* **K**.

Įrodymas. Kiekvieną lyginį skaičių $2m$ galima užrašyti šitaip: $2m=2^k s$; čia s nesidalija iš 2.

Kai k reikšmių aibė yra visi sveikieji neneigiami skaičiai, o s — visi teigiamieji nelyginiai skaičiai, tai $2^k s$ reikšmių aibė yra visi sveikieji neneigiami skaičiai.

Lemą įrodysime matematinės indukcijos metodu.

1) Jeigu $k=0$, tai $2^k s=2^0 s=s$ — nelyginis skaičius. Iš 1 lemos išplaukia, kad 2 lemos tvirtinimas teisingas, kai polinomas yra nelyginio laipsnio (realusis skaičius priklauso kompleksinių skaičių laukui). Taigi lemos tvirtinimas teisingas, kai $k=0$.

2) Tarkime, kad 2 lemos tvirtinimas teisingas visiems polinomams, kurių laipsnis yra $2^r s$ (kai $k=r$), s — bet koks nelyginis skaičius.

3) Įrodysime, kad, esant teisingai prielaidai, 2 lemos tvirtinimas teisingas visiems polinomams, kurių laipsnis yra $2^{r+1}t$, t – bet koks nelyginis skaičius (t. y. kai $k=r+1$).

Tarkime, kad $f(x)$ laipsnis lygus $2^{r+1}t$, t. y.

$$n=2^{r+1}t.$$

Pagal 76 paragrafo 151 teoremą egzistuoja lauko $\mathbf{R}$ plėtinys $\mathbf{R}'$ ($\mathbf{R}\subset\mathbf{R}'$), kuriame polinomas $f(x)$ turi n šaknų $l_1, \ldots, l_n$, t. y. teisinga lygybė (žiede $\mathbf{R}'[x]$)

$$f(x)=(x-l_1)\ldots(x-l_n), \quad a_n=1.$$

Užtenka įrodyti, kad bent vienas iš $l_1, \ldots, l_n$ yra kompleksinis skaičius. Imame realųjį skaičių c ir sudarome reiškinius

$$h_{ij}=l_il_j+c(l_i+l_j),$$

imdami i ir j poras, kai $i<j$.

Elementų h_{ij} yra

$$m=C_n^2=\frac{n(n-1)}{2}=\frac{1}{2}\,2^{r+1}t(2^{r+1}t-1)=2^rs;$$

čia $s=t(2^{r+1}t-1)$ – nelyginis skaičius.

Sudarome polinomą $g(x)$, kurio šaknys yra h_{ij} $(i<j)$, t. y.

$$g(x)=\prod_{1\leqslant i<j\leqslant n}(x-h_{ij})=x^m+b_{m-1}x^{m-1}+\ldots+b_1x+b_0.$$

To polinomo laipsnis yra $m=2^rs$, s – nelyginis, o jo koeficientai – n kintamųjų pagrindinių simetrinių polinomų reikšmės su atitinkamais ženklais taške h_{ij} $(1\leqslant i<j\leqslant n)$. Iš h_{ij} konstrukcijos išplaukia, kad $b_0, b_1, \ldots, b_{m-1}$ yra polinomo $f(x)$ šaknų $l_1, \ldots, l_n$ polinomai su realiaisiais koeficientais.

Iš h_{ij} išraiškų ir polinomo $g(x)$ išraiškos išeina, kad, vietoj $l_1, \ldots, l_n$ paėmus bet kurį jų kėlinį $l_{i_1}, \ldots, l_{i_n}$, polinomo $g(x)$ išraiškoje keičiasi tik daugiklių $(x-h_{ij})$ tvarka. Tai reiškia, kad polinomo $g(x)$ koeficientai nesikeičia keičiant šaknų $l_i, \ldots, l_n$ tvarką. Todėl polinomo $g(x)$ koeficientai $b_0, b_1, \ldots, b_{m-1}$ yra šaknų $l_1, \ldots, l_n$ simetriniai polinomai su realiaisiais koeficientais. Taigi iš Vieto formulių ir pagrindinės teoremos apie simetrinius polinomus išplaukia, jog $b_0, b_1, \ldots, b_{m-1}$ yra polinomo $f(x)$ koeficientų $a_0, a_1, \ldots, a_n$ polinomai su realiaisiais koeficientais, t. y. realieji skaičiai.

$g(x)$ yra polinomas su realiaisiais koeficientais, jo laipsnis $n=2^rs$, s – nelyginis skaičius. Pagal prielaidą jis turi šaknį kompleksinių skaičių lauke $\mathbf{K}$. Taigi, kad ir koks būtų realusis skaičius c, egzistuoja tokia indeksų i ir j $(1\leqslant i\leqslant n,\ 1\leqslant j\leqslant n)$ pora, kad

$$h_{ij}=l_il_j+c(l_i+l_j)$$

yra kompleksinis skaičius. Kadangi *realiųjų skaičių be galo daug, o skirtingų porų i, j yra baigtinis skaičius, tai egzistuoja bent du skirtingi realieji skaičiai c_1 ir c_2, kuriuos atitinka ta pati indeksų pora i_0, j_0.* Taigi, paėmę $c=c_1$ ir $c=c_2$ $(c_1\neq c_2)$, gauname du kompleksinius skaičius

$$h^{(1)}=l_{i_0}l_{j_0}+c_1(l_{i_0}+l_{j_0}), \quad h^{(2)}=l_{i_0}l_{j_0}+c_2(l_{i_0}+l_{j_0}).$$

Iš pastarųjų lygybių gauname

$$-p=l_{i_0}+l_{j_0}=\frac{h^{(1)}-h^{(2)}}{c_1-c_2}\in\mathbf{K},$$

$$q=l_{i_0}l_{j_0}=\frac{c_1h^{(2)}-c_2h^{(1)}}{c_1-c_2}\in\mathbf{K},$$

t. y. p ir q – kompleksiniai skaičiai. Iš Vieto teoremos išplaukia, kad l_{i_0} ir l_{j_0} yra polinomo

$$x^2+px+q\in\mathbf{K}[x]$$

šaknys. Kadangi 2-ojo laipsnio polinomo su kompleksiniais koeficientais šaknys yra kompleksiniai skaičiai, tai l_{i_0} ir l_{j_0} taip pat *kompleksiniai skaičiai.*

Iš to išplaukia, kad 2 lemos tvirtinimas teisingas, kai $k=r+1$. Telieka taikyti matematinės indukcijos principą.

Priminsime, kad kompleksiniam skaičiui α jungtinį skaičių žymime $\bar{\alpha}$.

3 lema. *Jeigu polinomas su realiaisiais koeficientais turi menamąją šaknį α, tai $\bar{\alpha}$ taip pat yra to polinomo šaknis.*

Įrodymas. Tarkime, kad

$$f(x)=\sum_{j=0}^{n}a_jx^j$$

yra polinomas su realiaisiais koeficientais, t. y. $a_j\in\mathbf{R}$, $j=0, 1, \ldots, n$.

Kadangi $f(\alpha)=0$, tai ir $\overline{f(\alpha)}=0$. Bet

$$0=\overline{f(\alpha)}=\overline{\sum_{j=0}^{n}a_j\alpha^j}=\sum_{j=0}^{n}\overline{a_j\alpha^j}=\sum_{j=0}^{n}\bar{a}_j\bar{\alpha}^j=\sum_{j=0}^{n}a_j\bar{\alpha}^j=f(\bar{\alpha}),$$

t. y.

$$f(\bar{\alpha})=0.$$

Tai ir reikėjo įrodyti.

4 lema. *Jeigu*

$$f(x)=\sum_{j=0}^{n}a_jx^j\in\mathbf{K}[x],\quad \bar{f}(x)=\sum_{j=0}^{n}\bar{a}_jx^j,$$

tai $g(x)=f(x)\bar{f}(x)\in\mathbf{R}[x]$.

Įrodymas. Sudauginę $f(x)$ ir $\bar{f}(x)$, gauname $g(x)=f(x)\bar{f}(x)$,

$$g(x)=\sum_{j=0}^{2n}b_jx^j,\quad b_j=\sum_{l+k=j}a_l\bar{a}_k,\quad j=0, 1, \ldots, 2n.$$

Įrodysime, kad polinomo $g(x)$ koeficientai yra realieji skaičiai. Rasime koeficientui b_j jungtinį skaičių

$$\overline{b}_j = \overline{\sum_{l+k=j} a_l a_k} = \sum_{l+k=j} \overline{a_j a_k} = \sum_{l+k=j} \bar{a}_l \bar{a}_k = \sum_{l+k=j} \bar{a}_l a_k = b_j.$$

Lygybės $b_j = \overline{b}_j$, $j=0, 1, \ldots, 2n$, reiškia, kad b_j yra realieji skaičiai.

Taigi $g(x) \in \mathbf{R}[x]$.

170 teorema (pagrindinė klasikinės algebros teorema). *Kiekvienas n-ojo* $(n \geqslant 1)$ *laipsnio polinomas* $f(x)$ *su kompleksiniais koeficientais kompleksinių skaičių lauke* $\mathbf{K}$ *turi n šaknų.*

Žiede $\mathbf{K}[x]$ *polinomo* $f(x)$ *kanoninis skaidinys yra*

$$f(x) = a_n (x-l_1)^{m_1} \ldots (x-l_k)^{m_k};$$

čia a_n *– vyriausiasis koeficientas,* $l_1, \ldots, l_k$ *– polinomo šaknys.*

Įrodymas. Naudodamiesi polinomu

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbf{K}[x], \quad n \geqslant 1,$$

sudarome polinomą $g(x) = f(x)\bar{f}(x) \in \mathbf{R}[x]$. Pagal 4 lemą $g(x)$ yra polinomas su realiaisiais koeficientais. Iš 2 lemos išplaukia, kad polinomas $g(x)$ turi šaknį $\alpha \in \mathbf{K}$, t. y. $g(\alpha) = 0$.

Taigi $g(\alpha) = f(\alpha)\bar{f}(\alpha) = 0$,

$$\bar{f}(\alpha) = \sum_{j=0}^{n} \bar{a}_j \alpha^j.$$

Kadangi lauke $\mathbf{K}$ nėra nulio daliklių, tai vienas iš daugiklių $f(\alpha)$ arba $\bar{f}(\alpha)$ lygus nuliui.

Jeigu $f(\alpha) = 0$, tai $\alpha \in \mathbf{K}$ yra polinomo $f(x)$ šaknis.

Jeigu

$$\bar{f}(\alpha) = 0,$$

tai

$$0 = \overline{0} = \overline{\bar{f}(\alpha)} = \overline{\sum_{j=0}^{n} \bar{a}_j \alpha^j} = \sum_{j=0}^{n} \overline{\bar{a}_j} \overline{\alpha^j} = \sum_{j=0}^{n} a_j \bar{\alpha}^j = f(\bar{\alpha}),$$

ir $\bar{\alpha} \in \mathbf{K}$ yra polinomo $f(x)$ šaknis.

Taigi įrodėme, kad $f(x) \in \mathbf{K}[x]$ turi šaknį $l_1 = \alpha \in \mathbf{K}$.

Gauname $f(x) = (x-l_1) f_1(x)$, $f_1(x) \in \mathbf{K}[x]$ yra $n-1$-ojo laipsnio polinomas. Iš šios teoremos įrodymo pirmosios dalies, kai $n-1>0$, išplaukia, kad egzistuoja $l_2 \in \mathbf{K}$, $f_1(l_2) = 0$, t. y. $f(x) = (x-l_1)(x-l_2) f_2(x)$, $f_2(x) \in \mathbf{K}[x]$ yra $n-2$-ojo laipsnio polinomas.

Taip samprotaudami toliau, po n žingsnių gausime

$$f(x)=a_n(x-l_1)(x-l_2)\ldots(x-l_n),\quad l_1,\ l_2,\ \ldots,\ l_n\in\mathbf{K}.$$

Sugrupavę vienodus daugiklius, gausime teoremoje minimą polinomo $f(x)$ kanoninį skaidinį.

Iš pagrindinės teoremos išplaukia šios išvados:

1) *žiede* $\mathbf{K}[x]$ *tik pirmojo laipsnio polinomai yra pirminiai*;

2) *laukas* $\mathbf{K}$ *algebriškai uždaras.*

Pastaba. Pagrindinės klasikinės algebros teoremos įrodymas nėra konstruktyvus. Juo remiantis negalima sukonstruoti algoritmo polinomo šaknims rasti.

§86. Polinomų su realiaisiais koeficientais kanoninis skaidinys

Išsiaiškinsime, kokio pavidalo kanoninį skaidinį turi polinomas $f(x)\in\mathbf{R}[x]$.

171 teorema. *Kiekvienas aukštesnio kaip antrojo laipsnio polinomas su realiaisiais koeficientais yra išskaidomas žiede* $\mathbf{R}[x]$.

Įrodymas. Tarkime, kad $f(x)$ yra n-ojo laipsnio ($n\geqslant 3$) polinomas su realiaisiais koeficientais. Tas polinomas turi šaknį $\alpha\in\mathbf{K}$ (žr. § 85, 2 lemą).

Jeigu $\alpha\in\mathbf{R}$, tai $f(x)=(x-\alpha)\,q(x)$ ir $x-\alpha\in\mathbf{R}[x]$, $q(x)\in\mathbf{R}[x]$. Taigi $f(x)$ yra sudėtinis žiede $\mathbf{R}[x]$ polinomas.

Jeigu $\alpha\notin\mathbf{R}$, tai $\bar{\alpha}$ irgi yra polinomo $f(x)$ šaknis (žr. § 85, 3 lemą). Todėl žiede $\mathbf{K}[x]$ teisinga išraiška

$$f(x)=(x-\alpha)(x-\bar{\alpha})\,g(x).$$

Bet $(x-\alpha)(x-\bar{\alpha})=x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$.

Pažymėję $\alpha=a+ib$, gauname $\bar{\alpha}=a-ib$, ir $\alpha+\bar{\alpha}=2a\in\mathbf{R}$, $\alpha\bar{\alpha}=a^2+b^2\in\mathbf{R}$, ir

$$(x-\alpha)(x-\bar{\alpha})=x^2-2ax+|\alpha|^2=f_1(x)\in\mathbf{R}[x].$$

Kadangi išraiškos $f(x)=g(x)f_1(x)$ polinomai $f(x)$, $f_1(x)$ priklauso $\mathbf{R}[x]$, tai ir $g(x)$ priklauso $\mathbf{R}[x]$. Todėl žiede $\mathbf{R}[x]$ polinomą $f(x)$ galima išreikšti dviejų polinomų sandauga.

Išvada. *n-ojo* ($n\geqslant 1$) *laipsnio polinomo* $f(x)\in\mathbf{R}[x]$ *žiede* $\mathbf{R}[x]$ *kanoninis skaidinys yra šitoks*:

$$f(x)=a_n\prod_{j=1}^{m_1}(x-l_j)^{s_j}\prod_{k=1}^{m_2}(x^2+p_kx+q_k)^{t_k};$$

čia $s_1+\ldots+s_{m_1}+2(t_1+\ldots+t_{m_2})=n$.

Įrodymas. Žiede $\mathbf{R}[x]$ pirminiai yra tik pirmojo laipsnio polinomai ir tie antrojo laipsnio polinomai, kurie neturi realiųjų šaknų. Išreiškę $f(x)$ pir-

minių virš $\mathbf{R}[x]$ polinomų sandauga ir atitinkamai sugrupavę pirmojo ir antrojo laipsnio daugiklius, gauname reikiamą skaidinį.

Atkreipsime dėmesį, kad virš racionaliųjų skaičių lauko yra bet kokio laipsnio pirminių polinomų (žr. Eizenšteino kriterijaus išvadą).

Uždaviniai

1. Išreikškite pirminių virš 1) racionaliųjų, 2) realiųjų, 3) kompleksinių skaičių lauko polinomų sandauga šiuos polinomus:

a) x^3-27; b) x^2-5x+6; c) x^6-16;

d) x^4+4; e) x^4-10x^2+1; f) x^8-2x^4+1.

2. Raskite žemiausio laipsnio polinomą su kompleksiniais koeficientais, kurio šaknys yra:

a) $1,\ -1,\ 2-i,\ 3+i$;

b) $3,\ \frac{1}{3},\ 1-i$ – kartotinė;

c) i – trečiojo kartotinumo, $1+2i,\ 3-i$.

3. Raskite žemiausio laipsnio polinomą su realiaisiais koeficientais, kurio šaknys yra:

a) $1,\ -1,\ 2-i$;

b) $2,\ \frac{1}{2},\ 2+i$ – kartotinė;

c) $2+i,\ 3-i$;

d) $-\frac{1}{3},\ 2+7i$ – kartotinės.

§87. Polinomo su sveikaisiais koeficientais racionaliųjų šaknų savybės ir jų radimo algoritmas

Kaip nustatyti, ar polinomas $g(x)$ su racionaliaisiais arba sveikaisiais koeficientais turi racionaliųjų šaknų ir, jeigu turi, tai kaip jas rasti? Spręsime abu tuos uždavinius.

Kadangi $g(x)=cf(x)$, $c\in\mathbf{Q}$, o $f(x)$ – primityvusis polinomas (su sveikaisiais koeficientais), tai toliau nagrinėsime tik primityviuosius polinomus.

172 teorema. *Jeigu nesuprastinama trupmena l/m* yra polinomo

$$f(x)=\sum_{j=0}^{n} a_j x^j$$

su sveikaisiais koeficientais šaknis, tai jo vyriausiasis koeficientas a_n dalijasi iš m, o laisvasis narys a_0 – iš l.

Įrodymas. Lygybę

$$f\left(\frac{l}{m}\right)=\sum_{j=0}^{n} a_j \left(\frac{l}{m}\right)^j=0$$

padauginę iš m^n ir pertvarkę, gauname lygybes

$$\sum_{j=1}^{n} a_j m^{n-j} l^j = -a_0 m^n \text{ ir } \sum_{j=0}^{n-1} a_j m^{n-j} l^j = -a_n l^n.$$

Kadangi D $(l, m)=1$, tai iš pastarųjų lygybių išplaukia, kad

$$l \mid a_0, \; m \mid a_n.$$

Tai ir reikėjo įrodyti.

Iš tos teoremos išplaukia ši išvada: *jeigu polinomo su sveikaisiais koeficientais vyriausiojo nario koeficientas lygus vienetui, tai polinomo racionaliosios šaknys (jeigu jos egzistuoja) yra sveikieji skaičiai ir laisvojo nario dalikliai.*

Remiantis ta išvada, labai paprastai galima rasti polinomo $f(x)=x^n+ +a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ su sveikaisiais koeficientais sveikąsias šaknis (trupmeninių šaknų jis neturi). Pirmiausia reikia rasti laisvojo nario a_0 visus daliklius, po to, naudojantis Hornerio schema, reikia patikrinti, kurie iš jų yra polinomo $f(x)$ šaknys.

Pavyzdys. Rasime polinomo

$$f(x)=x^3-2x^2-5x+6$$

racionaliąsias šaknis.

Kadangi vyriausiasis koeficientas lygus vienetui, tai polinomo šaknų reikia ieškoti tarp 6 daliklių.

Dalikliai yra ±1, ±2, ±3, ±6, t. y. iš viso 8. Naudodamiesi Hornerio schema, gauname $f(1)=0$, $f(-2)=0$, $f(3)=0$. Taigi polinomo šaknys yra 1, -2, 3.

Tuo atveju, kai polinomo vyriausiasis koeficientas nelygus vienetui, rasti racionaliąsias šaknis, remiantis tik 172 teorema, gana sudėtinga.

Kodėl taip yra, paaiškės iš pavyzdžio.

Pavyzdys. Rasime polinomo

$$f(x)=4x^4-9x^3-18x^2+29x-6$$

racionaliąsias šaknis.

1) Randame vyriausiojo nario daliklius m ir laisvojo nario daliklius l:

$$4=2\cdot2, \; m=\pm1, \; \pm2, \; \pm4,$$

$$6=2\cdot3, \; l=\pm1, \; \pm2, \; \pm3, \; \pm6.$$

2) Randame visas trupmenas l/m, kurių skaitiklis yra laisvojo nario daliklis, o vardiklis – vyriausiojo koeficiento daliklis:

$$l/m=\pm1, \; \pm2, \; \pm3, \; \pm6, \; \pm\frac{1}{4}, \; \pm\frac{3}{2}, \; \pm\frac{3}{4}, \; \pm\frac{1}{2}.$$

Gavome net 16 tokių trupmenų, tarp kurių reikia ieškoti polinomo šaknų. Norint patikrinti, kurios iš jų polinomo šaknys, tektų daug skaičiuoti. Naudosimės Hornerio schema:

a	4	-9	-18	29	-6
1	4	-5	-23	6	0
-1	4	-9	-14	20	
-2	4	-13	3	0	
3	4	-1	0		

Nustatėme, kad $l_1=1$, $l_2=-2$ ir $l_3=3$ yra polinomo šaknys. Radę tris šaknis, galime užrašyti

$$f(x)=(x-1)(x+2)(x-3)(4x-1).$$

Iš lygties $4x-1=0$ gauname ketvirtąją šaknį $l_4=\frac{1}{4}$.

Jeigu nežinotume to polinomo šaknų, tai mums tektų nemažai skaičiuoti, nes yra net 16 skaičių aibėje, kuriai priklauso polinomo racionaliosios šaknys. Ypač daug skaičiuoti gali tekti tada, kai polinomo laisvasis narys a_0 ir vyriausiasis koeficientas turi daug daliklių. Tada aibė

$$A_f=\left\{\frac{l}{m} \;\middle|\; l \mid a_0,\ m \mid a_n,\ \mathrm{D}(l, m)=1\right\}$$

turi daug elementų. Ją galima susiaurinti remiantis dar viena polinomo racionaliųjų šaknų savybe.

173 teorema. *Jeigu nesuprastinama trupmena l/m $(m>0)$ yra polinomo*

$$f(x)=\sum_{j=0}^{n} a_j x^j$$

su sveikaisiais koeficientais šaknis, tai su kiekvienu sveikuoju skaičiumi k, su kuriuo $l-km\neq 0$, polinomo $f(x)$ reikšmė taške k dalijasi iš $l-km$, t. y. $l-km \mid f(k)$.

Įrodymas. Polinomą $f(x)$ padauginę iš m^n, gauname

$$m^n f(x)=\sum_{j=0}^{n} (m^{n-j}a_j)(mx)^j.$$

Pažymėję $mx=y$, turime

$$m^n f(x)=g(y)=\sum_{j=0}^{n} (m^{n-j}a_j)y^j.$$

Kadangi $f\left(\frac{l}{m}\right)=0$, tai $g(l)=0$. Taigi $g(y)=(y-l)\,q(y)$; čia $q(y)$ – polinomas su sveikaisiais koeficientais. Įrašę į tą lygybę $y=km$, gauname

$$g(km)=m^n f(k)=(km-l)\,q(km).$$

Taigi

$$\frac{m^n f(k)}{l-km}=-q(km)$$

yra sveikasis skaičius, kai $l-km\neq 0$.

Užtenka įrodyti, kad $\mathrm{D}(m^n,\ l-km)=1$.

Žinome, kad $\mathrm{D}(l,\ m)=1$. Jeigu būtų $\mathrm{D}(l-km,\ m)>1$, tai trupmena

$$\frac{l-km}{m}$$

būtų suprastinama, t. y.

$$\frac{l-km}{m}=\frac{l'}{m'},\quad 0<m'<m.$$

Iš pastarosios lygybės gautume išraišką

$$\frac{l}{m}=\frac{l'}{m'}+k=\frac{l'+km'}{m'},$$

kuri reikštų, kad $\mathrm{D}(l,\ m)>1$, bet tai prieštarauja sąlygai $\mathrm{D}(l,\ m)=1$. Todėl $\mathrm{D}(l-km,\ m)=1$. Tuomet $\mathrm{D}(l-km,\ m^n)=1$ ir trupmena

$$\frac{m^n}{l-km}$$

yra nesuprastinama. Taigi $f(k)$ dalijasi iš $l-km$.

Iš tų abiejų teoremų išplaukia šitoks polinomo su sveikaisiais koeficientais

$$f(x)=\sum_{j=0}^{n} a_j x^j$$

racionaliųjų šaknų radimo algoritmas.

Sukonstruojame aibę $A_f=\left\{\frac{l}{m}\ \middle|\ l\mid a_0,\ m\mid a_n,\ \mathrm{D}(l,\ m)=1\right\}$. Pagal 172 teoremą polinomo $f(x)$ visos racionaliosios šaknys yra toje aibėje. 173 teorema teigia, kad polinomo visos racionaliosios šaknys yra aibėje

$$A_f^{(k_1,\ \ldots,\ k_r)}=\left\{\frac{l}{m}\ \middle|\ l\mid a_0,\ m\mid a_n,\ \mathrm{D}(l,\ m)=1,\ l-k_i m\mid f(k_i),\ i=1,\ \ldots,\ r\right\}.$$

Aišku, kad

$$A_f^{(k_1,\ \ldots,\ k_r)}\subset\ldots\subset A_f^{(k_1,\ k_2)}\subset A_f^{(k_1)}\subset A_f,\quad r\geqslant 2.$$

Parinkdami k_1, k_2, ..., k_r, procesą tęsiame tol, kol aibėje $A_f^{(k_1,\ \ldots,\ k_r)}$ liks „nedaug“ elementų. Tada tikrinimo būdu randame polinomo $f(x)$ racionaliąsias šaknis arba nustatome, kad jų nėra.

Pavyzdys. Rasime polinomo

$$f(x)=8x^4+22x^3-5x^2-28x+12$$

racionaliąsias šaknis.

Kadangi $8=2\cdot 2\cdot 2$, tai $m=\pm 1,\ \pm 2,\ \pm 4,\ \pm 8$, $12=2\cdot 2\cdot 3$ ir $l=\pm 1,\ \pm 2,\ \pm 4,\ \pm 3,\ \pm 6,\ \pm 12$, todėl

$$A_f=\left\{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12,\ \pm\frac{1}{2},\ \pm\frac{1}{4},\ \pm\frac{1}{8},\ \pm\frac{3}{2},\ \pm\frac{3}{4},\ \pm\frac{3}{8}\right\}.$$

Paėmę $k=1$, gauname $f(k)=f(1)=9$. Patikrinę, ar 9 dalijasi iš $l-m$, gauname

$$A_f^{(1)}=\left\{2,\ -2,\ 4,\ \frac{1}{2},\ -\frac{1}{2},\ \frac{1}{4},\ -\frac{1}{8},\ \frac{3}{2},\ \frac{3}{4}\right\}.$$

Ši aibė turi tik 9 elementus. Paėmę $k=-1$, gauname $f(-1)=21$. Patikrinę, ar 21 dalijasi iš $l-km=l+m$, gauname

$$A_f^{(1,\,-1)}=\left\{\pm 2,\ \frac{1}{2},\ -\frac{1}{2},\ -\frac{1}{8},\ \frac{3}{4}\right\}.$$

Pastarąsias 6 reikšmes tikriname naudodamiesi Hornerio schema:

l/m	8	22	-5	-28	12
-2	8	6	-17	6	0
-2	8	-10	3	0	
$\frac{1}{2}$	8	-6	0		
$\frac{3}{4}$	8	0			

Taigi polinomas turi 4 racionaliąsias šaknis: $l_1=l_2=-2$, $l_3=\frac{1}{2}$, $l_4=\frac{3}{4}$;

$$f(x)=8(x+2)^2\left(x-\frac{1}{2}\right)\left(x-\frac{3}{4}\right)=(x+2)^2(2x-1)(4x-3).$$

Uždaviniai

4. Raskite polinomų racionaliąsias šaknis ir išskaidykite šiuos polinomus žiede $\mathbf{Z}[x]$:

a) x^4-5x^2+4;
b) $x^3-11x^2+38x-40$;
c) $2x^4+11x^3-4x^2+11x-6$;
d) $6x^4+x^3+2x^2-4x+1$;
e) $7x^4-4x^3-66x^2+36x+27$;
f) $24x^5-110x^4+199x^3-196x^2+110x-21$.

§88. Algebrinės lygtys

Iš klasikinės algebros pagrindinės teoremos išplaukia, kad kiekvienas nenulinio laipsnio polinomas su kompleksiniais koeficientais turi tiek kompleksinių šaknų (kiekviena šaknis skaičiuojama tiek kartų, koks yra jos kartotinumas), koks yra jo laipsnis.

n-ojo laipsnio polinomo $f(x)$ *šaknys yra lygties*

$$f(x)=0$$

sprendiniai. Ta lygtis vadinama *algebrine n-ojo laipsnio lygtimi.* Todėl, norint rasti polinomo šaknis, reikia spręsti algebrinę lygtį.

Nėra bendro metodo visoms algebrinėms lygtims spręsti, tačiau yra būdų kai kurių lygčių sprendiniams rasti. Šiame paragrafe trumpai apžvelgsime tuos tipus polinomų, kurių šaknis galima rasti, išvardysime jau žinomus sprendimo metodus ir išnagrinėsime naujus.

Vadovėlio I dalies trečiojo skyriaus 45 paragrafe aiškinomės, kaip sprendžiamos antrojo, trečiojo ir ketvirtojo laipsnio algebrinės lygtys. Žinome, kad kiekvieno polinomo, kurio laipsnis ne didesnis už 4, šaknis galima rasti atlikus sudėties, atimties, daugybos, dalybos ir šaknies traukimo veiksmus su polinomo koeficientais. Tuo atveju, kai polinomo laipsnis didesnis už 4, nėra bendrųjų formulių nei bendrojo metodo polinomo šaknims rasti. Trumpai aptarsime tuos tipus polinomų (algebrinių lygčių), kurių šaknis galima rasti.

1. *Polinomo* ax^n+b, *kai* $n\geqslant 2$, *šaknys randamos iš formulių*

$$l_{k+1}=\left(\sqrt[n]{-\frac{b}{a}}\right)_k,\ k=0,\ 1,\ \ldots,\ n-1$$

(žr. 1 d., III skyr., § 43).

2. *Polinomų*

$$ax^{2m}+bx^m+c,$$

$$ax^{3m}+bx^{2m}+cx^m+d,$$

$$ax^{4m}+bx^{3m}+cx^{2m}+dx^m+h,\ \ m\in\mathbf{N},$$

šaknis taipogi galime rasti.

Atlikę keitinį $x^m=Y$, gauname polinomus

$$ay^2+by+c,$$

$$ay^3+by^2+cy+d,$$

$$ay^4+by^3+cy^2+dy+h,$$

kurių šaknis rasime išsprendę antrojo, trečiojo ir ketvirtojo laipsnio lygtis. Iš to išplaukia šitokie teiginiai:

2.1. *Lygtis*

$$ax^{2m}+bx^m+c=0$$

ekvivalenti lygčių visumai

$$\left[\begin{array}{l} x^m=t_1,\\ x^m=t_2; \end{array}\right.$$

čia t_1, t_2 — *lygties* $ay^2+by+c=0$ *sprendiniai.*

2.2. *Lygtis*

$$ax^{3m}+bx^{2m}+cx^m+d=0$$

ekvivalenti lygčių visumai

$$\left[\begin{array}{l} x^m=u_1, \\ x^m=u_2, \\ x^m=u_3; \end{array}\right.$$

čia u_1, u_2, u_3 — *lygties* $ay^3+by^2+cy+d=0$ *sprendiniai.*

2.3. *Lygtis*

$$ax^{4m}+bx^{3m}+cx^{2m}+dx^m+h=0$$

ekvivalenti lygčių visumai

$$\left[\begin{array}{l} x^m=v_1, \\ x^m=v_2, \\ x^m=v_3, \\ x^m=v_4; \end{array}\right.$$

čia v_1, v_2, v_3, v_4 — *lygties* $ay^4+by^3+cy^2+dy+h=0$ *sprendiniai.*

Pavyzdys. Išspręsime lygtį

$$x^9+x^6+x^3+1=0.$$

Kadangi lygties $y^3+y^2+y+1=0$ sprendiniai yra -1, i, $-i$, tai pradinė lygtis ekvivalenti lygčių visumai

$$\left[\begin{array}{l} x^3=-1, \\ x^3=i, \\ x^3=-i. \end{array}\right.$$

Išsprendę tas lygtis, gauname:

$$l_{k+1}=(\sqrt[3]{-1})_k, \quad k=0,\ 1,\ 2; \quad l_1=\frac{1}{2}+i\,\frac{\sqrt{3}}{2},$$

$$l_2=-1,$$

$$l_3=\frac{1}{2}-i\,\frac{\sqrt{3}}{2};$$

$$l_{3+k+1}=(\sqrt[3]{i})_k, \quad k=0,\ 1,\ 2; \quad l_4=\frac{\sqrt{3}}{2}+i\,\frac{1}{2},$$

$$l_5=-\frac{\sqrt{3}}{2}+i\,\frac{1}{2},$$

$$l_6=-i;$$

$$l_{6+k+1}=(\sqrt[3]{-i})_k, \quad k=0,\ 1,\ 2; \quad l_7=i,$$

$$l_8=-\frac{\sqrt{3}}{2}-i\,\frac{1}{2},$$

$$l_9=\frac{\sqrt{3}}{2}-i\,\frac{1}{2}.$$

3. *Kai polinomo* $f(x)$ *koeficientai yra sveikieji (arba racionalieji) skaičiai ir polinomas turi racionaliąsias šaknis* $l_1, \ldots, l_m$, *o daugiklis* $g(x)$ *išraiškoje*

$$f(x)=g(x)\prod_{j=1}^{m}(x-l_j)$$

yra ne aukštesnio kaip 4*-ojo laipsnio arba kai jis yra* 1 *ar* 2 *atveju aptarto pavidalo, tada polinomo* $f(x)$ *šaknis galima rasti.* Tuo atveju racionaliąsias šaknis $l_1, \ldots, l_m$ randame žinomu racionaliųjų šaknų radimo metodu (žr. § 87), o kitas šaknis – išsprendę lygtį $g(x)=0$.

Pavyzdys. Rasime polinomo

$$f(x)=3x^6-16x^5+24x^4+15x^3-90x^2+34x+60$$

šaknis.

Kadangi polinomo koeficientai yra sveikieji skaičiai, tai pirmiausia randame jo racionaliąsias šaknis:

$$l_1=3,\quad l_2=-\frac{2}{3}.$$

Išskyrę tiesinius daugiklius $x-3$ ir $3x+2$, gauname išraišką

$$f(x)=(x-3)(3x+2)(x^4-3x^3+3x^2+6x-10).$$

Ketvirtojo laipsnio algebrinės lygties sprendimo metodu randame polinomo

$$g(x)=x^4-3x^3+3x^2+6x-10$$

šaknis:

$$\sqrt{2},\ -\sqrt{2},\ \frac{3+i\sqrt{11}}{2},\ \frac{3-i\sqrt{11}}{2}.$$

Taigi polinomo $f(x)$ šaknys yra

$$-\frac{3}{2},\ 3,\ \sqrt{2},\ -\sqrt{2},\ \frac{3+i\sqrt{11}}{2},\ \frac{3-i\sqrt{11}}{2}.$$

4. *Kai polinomo* $f(x)$ *kartotinių ir paprastų daugiklių laipsniai ne didesni už* 4 *arba kai tie daugikliai yra bent vieno anksčiau išvardytų polinomų pavidalo, tada jo šaknis irgi galime rasti, nes mokame rasti kartotinius daugiklius* (žr. § 78) *ir tų daugiklių šaknis, kai jie yra nurodyto pavidalo.*

Tuo atveju lygtis $f(x)=0$ atrodo šitaip:

$$g_1(x)\left(g_2(x)\right)^2\ldots\left(g_m(x)\right)^m=0.$$

Jos sprendinius rasime išsprendę lygčių visumą

$$\left[\begin{array}{l} g_1(x)=0,\\ g_2(x)=0,\\ \cdots\cdots\\ g_m(x)=0. \end{array}\right.$$

Reikia tik atsiminti, kad polinomo $g_s(x)$ kiekviena šaknis yra polinomo $f(x)$ s-ojo kartotinumo šaknis.

Pavyzdys. Išskyrę polinomo

$$f(x)=2x^7-x^6+2x^5-x^4-2x^3+x^2-2x+1$$

kartotinius daugiklius, gauname

$$f(x)=(2x^3-x^2-2x+1)(x^2+1)^2.$$

Todėl polinomo šaknis randame išsprendę dviejų lygčių visumą

$$\begin{cases} 2x^3-x^2-2x+1=0, \\ x^2+1=0. \end{cases}$$

Pirmosios lygties sprendiniai yra 1, -1, $\frac{1}{2}$, o antrosios $-i$ ir $-i$. Polinomas $f(x)$ turi paprastąsias šaknis 1, -1, $\frac{1}{2}$ ir antrojo kartotinumo šaknis i ir $-i$.

5. Sangrąžiniai polinomai (sangrąžinės lygtys).

Polinomą $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0$ vadiname *pirmojo tipo sangrąžiniu polinomu, jeigu vienodai nuo galų nutolę jo koeficientai yra lygūs*, t. y. $a_n=a_0$, $a_{n-1}=a_1$, ..., $a_{n-k}=a_k$ $(k=0, 1, \ldots, n)$; žymime $f_+(x)$. *Jeigu vienodai nuo galų nutolę koeficientai skiriasi tik ženklu*, t. y. $a_n=-a_0$, $a_{n-1}=-a_1$, ..., $a_{n-k}=-a_k$ $(k=0, 1, \ldots, n)$, *tai tą polinomą vadiname antrojo tipo sangrąžiniu polinomu* ir žymime $f_-(x)$. Atitinkamos lygtys $f_+(x)=0$ ir $f_-(x)=0$ vadinamos *sangrąžinėmis algebrinėmis lygtimis.*

5a. Kai polinomo $f_-(x)$ laipsnis $n=2m$, tai, paėmę $k=m$, gauname $a_{2m-m}=-a_m$, t. y. $a_m=-a_m$, arba $a_m=0$. Todėl lygtį

$$f_-(x)=0,$$

atitinkamai sutvarkę narius, galime užrašyti šitaip:

$$\sum_{j=0}^{m-1} a_j x^j (x^{n-2j}-1)=0.$$

Kadangi

$$x^{n-2j}-1=(x-1)\sum_{l=n-1-2j}^{0} x^l,$$

tai lygtis turi sprendinį $x=1$. Iš Hornerio schemos išplaukia, kad

$$f_-(x)=(x-1)f_1(x);$$

čia $f_1(x)$ – pirmojo tipo sangrąžinis polinomas, kurio laipsnis lygus $2m-1$, o koeficientai yra

$$c_k=c_{2m-1-k}=\sum_{j=0}^{k} a_j, \quad k=0, 1, \ldots, m; \quad a_m=0.$$

Lygties $f_-(x)=0$, kai $n=2m$, kiti sprendiniai sutampa su pirmojo tipo sangrąžinės lygties $f_1(x)=0$ sprendiniais.

5b.c. Nagrinėsime lygtis

$$f_-(x)=0 \quad \text{ir} \quad f_+(x)=0,$$

kai jų laipsniai lygūs $2m-1$. Šiuo atveju tas lygtis galime užrašyti šitaip:

$$\sum_{j=0}^{m-1} a_j x^j (x^{n-2j}-1)=0, \quad \sum_{j=0}^{m-1} a_j x^j (x^{n-2j}+1)=0.$$

Matome, kad pirmosios lygties sprendinys yra $x=1$ ir $f_-(x)=(x-1)f_1(x)$; čia $f_1(x)$ – sangrąžinis polinomas, kurio laipsnis yra $2m-2$.

Kadangi

$$x^{n-2j}+1=(x+1)\sum_{l=n-2j-1}^{0}(-1)^l x^l,$$

kai $n-2j$ – nelyginis, tai antroji lygtis turi sprendinį $x=-1$. Iš Hornerio schemos gauname $f_+(x)=(x+1)g_1(x)$; čia $g_1(x)$ – antrojo tipo sangrąžinis polinomas, kurio laipsnis yra $2m-2$, t. y. lygtį $f_+(x)=0$ sprendžiame taip pat kaip ir **5a** atveju.

5d. Lieka išsiaiškinti, kaip sprendžiama lygtis

$$f_+(x)=0,$$

kai deg $(f_+)=2m$.

Šiuo atveju lygtį galime užrašyti šitaip:

$$x^m\left(\sum_{j=0}^{m-1} a_j\left(x^{m-j}+\frac{1}{x^{m-j}}\right)+a_m\right)=0.$$

Kadangi $x=0$ nėra polinomo šaknis, tai pastaroji lygtis ekvivalenti lygčiai

$$\sum_{j=0}^{m-1} a_j\left(x^{m-j}+\frac{1}{x^{m-j}}\right)+a_m=0.$$

Iš keitinio $x+\frac{1}{x}=z$ gauname

$$\left(x+\frac{1}{x}\right)^2=\left(x^2+\frac{1}{x^2}\right)+2,$$

t. y.

$$x^2+\frac{1}{x^2}=z^2-2,$$

ir apskritai

$$z^l=\left(x+\frac{1}{x}\right)^l=$$

$$=\left(x^l+\frac{1}{x^l}\right)+C_l^1\left(x^{l-2}+\frac{1}{x^{l-2}}\right)+\ldots+\begin{cases} C_l^{(l-1)/2}\left(x+\frac{1}{x}\right), & \text{kai } l=2r+1, \\ C_l^{l/2}, & \text{kai } l=2r. \end{cases}$$

Todėl $x^{m-j}+\frac{1}{x^{m-j}}=h_{m-j}(z)$; čia $h_{m-j}(z)$ – kintamojo z polinomas, kurio laipsnis lygus $m-j$. *Įrašę tas išraiškas į lygtį, gauname algebrinę lygtį* $g(z)=0$, *kurios laipsnis dvigubai mažesnis už pradinės lygties* $f_+(x)=0$ *laipsnį.*

Taigi kiekvienos sangrąžinės lygties, radę jos sprendinius 1 arba (ir) -1, laipsnį galime sumažinti dvigubai. Jeigu gautosios lygties

$$g(z)=0$$

polinomas $g(z)$ yra $1-4$ tipų, tai ir sangrąžinio polinomo $f(x)$ visas kitas šaknis rasime išsprendę visumą lygčių

$$x+\frac{1}{x}=t_i, \quad i=1, 2, \ldots, m;$$

čia t_i – lygties $g(z)=0$ sprendiniai.

Pavyzdys. Lygtis

$$f(x)=x^6+3x^5-5x^4+5x^2-3x-1=0$$

yra antrojo tipo sangrąžinė lygtis. Užpildę Hornerio lentelę

l	1	3	−5	0	5	−3	−1
1	1	4	−1	−1	4	1	0
−1	1	3	−4	3	1	0	

gauname išraišką $f(x)=(x-1)(x+1)(x^4+3x^3-4x^2+3x+1)$ ir šaknis $l_1=1$, $l_2=-1$. Kitos šaknys yra 1-ojo tipo 4 laipsnio lygties

$$x^4+3x^3-4x^2+3x+1=0$$

sprendiniai.

Taigi

$$x^4+3x^3-4x^2+3x+1=x^2\left(\left(x^2+\frac{1}{x^2}\right)+3\left(x+\frac{1}{x}\right)-4\right).$$

Atlikę keitinį $x+\frac{1}{x}=z$, gauname $x^2+\frac{1}{x^2}=z^2-2$ ir polinomą

$$g(z)=z^2+3z-6,$$

kurio šaknys yra

$$t_1=\frac{-3-\sqrt{33}}{2}, \quad t_2=\frac{-3+\sqrt{33}}{2}.$$

Todėl kitas polinomo $f(x)$ šaknis randame išsprendę lygtis

$$x+\frac{1}{x}=\frac{-3-\sqrt{33}}{2}; \quad x+\frac{1}{x}=\frac{-3+\sqrt{33}}{2}.$$

Gauname

$$l_{3,4}=-\frac{1}{2}(3+\sqrt{33}\mp\sqrt{26+6\sqrt{33}}),$$

$$l_{5,6}=-\frac{1}{2}(3-\sqrt{33}\mp i\sqrt{6\sqrt{33}-26}).$$

Uždaviniai

5. Išspręskite lygtis:

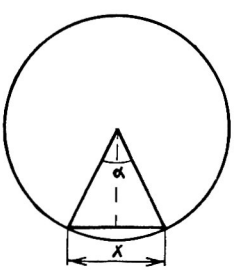
a) $2x^4-3x^2+1=0$;
b) $x^4-7x^2+10=0$;
c) $x^8-5x^4+4=0$;
d) $2x^6+11x^3-6=0$;
e) $7x^8-4x^4-3=0$;
f) $x^6-11x^4+38x^2-40=0$;
g) $x^4-2x^3-x^2-2x+1=0$;
h) $x^7-2x^6+3x^5-x^4-x^3+3x^2-2x+1=0$.

6. Išspręskite lygtį $f(x)=0$. Išreikškite pirminių polinomų virš laukų 1) **Q**, 2) **R**, 3) **K** sandauga šiuos polinomus:

a) $f(x)=6x^7-29x^6+11x^5+67x^4-51x^3-81x^2+9x+18$;
b) $f(x)=8x^7-4x^6-26x^5+29x^4-8x^3-16x^2+11x+6$;
c) $f(x)=6x^7-25x^6+5x^5-6x^4-51x^3+55x^2-50x+24$.

§89. Polinomo su realiaisiais koeficientais realiųjų šaknų apytikslio radimo uždavinys

Polinomo su realiaisiais koeficientais šaknų radimas turi ne tik teorinę, bet ir praktinę reikšmę. Taip, pavyzdžiui, *Leverje* (U. J. J. Leverrier, 1811–1877, prancūzų astronomas), norėdamas įrodyti Neptūno egzistavimą, sprendė lygtį



1 pav.

$$3447x^6+14560x^5+22430x^4+25857x^3+$$
$$+29193x^2+11596x+5602=0.$$

Konstruojant taisyklinguosius daugiakampius, taip pat reikia spręsti algebrines lygtis. Pavyzdžiui, norint į spindulio R skritulį įbrėžti taisyklingąjį n-kampį, reikia rasti jo kraštinės ilgį $x=2R\sin\frac{\pi}{n}$ (žr. 1 pav.).

Naudodamiesi formulėmis

$$(\cos\varphi+i\sin\varphi)^n=\cos n\varphi+i\sin n\varphi$$

ir

$$(\cos\varphi + i\sin\varphi)^n = \sum_{k=0}^{n} c_n^k (\cos\varphi)^{n-k} (i\sin\varphi)^k =$$

$$= \sum_{r=0}^{\left[\frac{n}{2}\right]} C_n^{2r} (-1)^r (\sin\varphi)^{2r} (\cos\varphi)^{n-2r} +$$

$$+ i \sum_{r=0}^{\left[\frac{n-1}{2}\right]} C_n^{2r+1} (-1)^r (\sin\varphi)^{2r+1} (\cos\varphi)^{n-(2r+1)}$$

(kai $n=2m+1$ – nelyginis, tada

$$n-(2r+1) = 2m+1-2r-1 = 2(m-r)$$

yra lyginis), gauname, kai $\varphi = \frac{\pi}{n}$,

$$\sum_{r=0}^{\left[\frac{n-1}{2}\right]} C_n^{2r+1} (-1)^r \left(\sin\frac{\pi}{n}\right)^{2r+1} \left(1-\sin^2\frac{\pi}{n}\right)^{m-r} = \sin\left(n\frac{\pi}{n}\right) = 0.$$

Kadangi $\sin\frac{\pi}{n} = \frac{x}{2R}$, o $1-\sin^2\frac{\pi}{n} = 1-\frac{x^2}{4R^2}$, tai x yra lygties

$$\sum_{r=0}^{\left[\frac{n-1}{2}\right]} C_n^{2r+2} (-1)^r \left(\frac{x}{2R}\right)^{2r+1} \left(1-\frac{x^2}{4R^2}\right)^{m-r} = 0$$

sprendinys, t. y. n-ojo laipsnio polinomo šaknis. Kai $n=2m$, tai, pažymėję $y=\cos\frac{\pi}{n}$, gauname

$$\sin^2\frac{\pi}{n} = 1-y^2$$

ir

$$\sum_{r=0}^{m} C_n^{2r} (-1)^r (1-y^2)^r y^{n-2r} = \cos\left(n\frac{\pi}{n}\right) = -1.$$

Taigi $x=2R\sin\frac{\pi}{n} = 2R\sqrt{1-y^2}$; čia y yra lygties

$$\sum_{j=0}^{m} (-1)^j C_n^{2j} y^{n-2j} (1-y^2)^j = -1$$

sprendinys, t. y. n-ojo laipsnio polinomo šaknis.

Nustatėme, kad *į spindulio R skritulį įbrėžto taisyklingojo n-kampio kraštinė x išreiškiama tam tikro n-ojo laipsnio polinomo šaknimi arba yra jo šaknis.*

Yra ir daugiau uždavinių, kuriuos sprendžiant reikia ieškoti polinomo šaknų.

Kadangi ne visada galima rasti polinomo realiąsias šaknis, tai reikia mokėti bent apytiksliai jas apskaičiuoti.

Norint rasti polinomo $f(x)$ su realiaisiais koeficientais realiųjų šaknų apytiksles reikšmes, reikia:

1) *nustatyti, ar polinomas turi realiųjų šaknų ir kiek jų turi,*

2) *atskirti šaknis, t. y. nustatyti intervalus (kuo mažesnius), kuriuose yra tik po vieną realiąją polinomo šaknį,*

3) *apskaičiuoti šaknis norimu tikslumu, t. y. žinoti būdą racionaliųjų skaičių sekos, kurios riba yra šaknis iš nustatytojo intervalo, nariams apskaičiuoti ir paklaidai įvertinti.*

Pirmieji du uždaviniai, t. y. realiųjų šaknų skaičiaus nustatymas ir jų atskyrimas, glaudžiai susiję. Kituose paragrafuose nagrinėsime kai kuriuos tų uždavinių sprendimo būdus.

§90. Intervalo, kuriame yra visos realiosios polinomo šaknys, ribų nustatymas

Šiame ir tolesniuose šio skyriaus paragrafuose laikysime, kad polinomas

$$f(x)=\sum_{j=0}^{n} a_j x^j,\quad a_j\in\mathbf{R},\quad j=0,\ 1,\ \ldots,\ n,$$

neturi kartotinių šaknų ir jo vyriausiasis koeficientas a_n teigiamas.

Jeigu polinomas turėtų kartotinių šaknų, tai jis turėtų ir kartotinių daugiklių. Tuo atveju, pritaikę kartotinių daugiklių atskyrimo metodą, polinomą užrašytume šitaip:

$$f(x)=g_1(x)\left(g_2(x)\right)^2\ldots\left(g_m(x)\right)^2$$

ir vietoj polinomo $f(x)$ nagrinėtume polinomus $g_1(x)$, $g_2(x)$, ..., $g_m(x)$, kurie neturi kartotinių šaknų. Tų polinomų šaknys sutampa su polinomo $f(x)$ šaknimis ir juos būtų paprasčiau nagrinėti, nes jų laipsniai žemesni už polinomo $f(x)$ laipsnį.

Reikalavimas, kad būtų $a_n>0$, nemažina bendrumo, nes polinomų $f(x)$ ir $-f(x)$ šaknys sutampa.

Jeigu iš anksto nėra žinoma, kad $f(x)$ neturi kartotinių šaknų, tai tą reikia patikrinti skaičiuojant polinomo $f(x)$ ir jo išvestinės $f'(x)$ d.b.d. $(D(f, f')=1)$ arba polinomo diskriminantą $D(f)$.

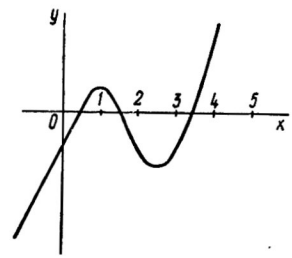
Kadangi *polinomas su realiaisiais koeficientais apibrėžia tolydžią realaus kintamojo x, $x\in\mathbf{R}$, funkciją, tai jo šaknys yra tos x reikšmės (taškai), kuriose $f(x)$ grafikas kerta x ašį.*

Todėl apytikslį vaizdą apie realiųjų šaknų skaičių ir jų išsidėstymą galime susidaryti nagrinėdami polinominės funkcijos $f(x)$ grafiką. Pavyzdžiui,

iš 5-ojo laipsnio polinominės funkcijos $f(x)$ grafiko (2 pav.) nustatome, kad polinomo realiosios šaknys yra intervaluose [0, 1], [1, 2] ir [3, 4].

x	-1	0	1	2	3	4
$f(x)$	-3	-1	$2/3$	-1	-1	2

Tačiau negalime tvirtinti, kad nėra daugiau realiųjų šaknų, nes grafikas gali būti nubrėžtas netiksliai. Norėdami patikslinti grafiką, turime imti daugiau x reikšmių, bet ir tuomet galime padaryti klaidų. Tikslus vaizdas bus tik tada, kai realiųjų šaknų skaičius bus lygus polinomo laipsniui ir grafikas tiek pat kartų kirs x ašį (t. y. jei paveiksle būtų pateiktas trečiojo laipsnio polinominės funkcijos grafikas).



2 pav.

Tačiau jeigu, pavyzdžiui, nustatėme, kad $f(x)>0$, kai $x\geqslant 4$, ir $f(x)<0$, kai $x\leqslant 0$, tai reiškia, kad visos realiosios polinomo $f(x)$ šaknys yra intervale [0, 4].

Bendruoju atveju intervalą, kuriame yra visos realiosios polinomo $f(x)$ šaknys, galima nustatyti remiantis šiomis teoremomis.

174 teorema. *Žymėsime* $A=\max\{|a_0|, \ldots, |a_{n-1}|\}$. *Visos polinomo*

$$f(x)=\sum_{j=0}^{n} a_j x^j,\quad a_j\in\mathbf{R},\quad j=0, 1, \ldots, n,$$

realiosios šaknys yra intervale $[-M, M]$; *čia*

$$M=1+\frac{A}{|a_n|}.$$

Įrodymas. Užtenka nustatyti, kad $|f(x)|>0$, kai $|x|>M$. Todėl vertiname polinominės funkcijos $f(x)$ modulį $|f(x)|$ iš apačios:

$$|f(x)|=\left|\sum_{j=0}^{n} a_j x^j\right|=\left|a_n x^n+a_n\sum_{j=0}^{n-1}\frac{a_j}{a_n}x^j\right|\geqslant$$

$$\geqslant|a_n||x^n|-|a_n|\sum_{j=0}^{n-1}\frac{|a_j|}{|a_n|}|x|^j\geqslant|a_n|\left(|x|^n-\frac{A}{|a_n|}\sum_{j=0}^{n-1}|x|^j\right)=$$

$$=|a_n|\left(|x|^n-\frac{A}{|a_n|}\,\frac{|x|^n-1}{|x|-1}\right),\quad |x|>1.$$

Kai $|x|>M$, tai $|x|-1>\frac{A}{|a_n|}$ ir

$$|f(x)|\geqslant|a_n|\left(|x|^n-(|x|^n-1)\right)=|a_n|>0.$$

Pastaroji nelygybė reiškia, kad $f(x)\neq 0$, kai $|x|>M$, t. y. už intervalo $[-M, M]$ $f(x)$ reikšmės niekur nelygios nuliui. Tai ir įrodo teoremos tvirtinimą.

Pavyzdys. Polinomo $f(x)=3x^7-6x^6+4x^5-12x^4+7x^3+9$ realiosios šaknys, jeigu jos egzistuoja, priklauso intervalui $[-5, 5]$, nes $A=12$, $a_n=3$ ir $M=1+\frac{A}{|a_n|}=1+4=5$.

175 teorema. *Polinomo*

$$f(x)=\sum_{j=0}^{n} a_j x^j,\quad a_j\in\mathbf{R},\quad j=0,\ 1,\ \ldots,\ n,$$

su teigiamu vyriausiuoju koeficientu ($a_n>0$) *visos teigiamosios šaknys mažesnės už skaičių*

$$N=1+\sqrt[m]{\frac{A_1}{a_n}};$$

čia a_{n-m} *— pirmasis neigiamas narys sekoje* $a_n, a_{n-1}, \ldots, a_2, a_1, a_0$, *o* A_1 *— neigiamų koeficientų modulio maksimumas, t. y.*

$$A_1=\max_{a_j<0}\{|a_j|\}.$$

Įrodymas. Teoremos tvirtinimas išplaukia iš nelygybės

$$f(x)\geqslant a_n\left(\sum_{a_j>0}\frac{a_j}{a_n}x^j-\frac{1}{a_n}\max_{a_j<0}\{|a_j|\}\sum_{j=0}^{n-m}x^j\right)\geqslant$$

$$\geqslant a_n\left(x^n-\frac{A_1}{a_n}\,\frac{x^{n-m+1}-1}{x-1}\right),\quad x>1,$$

iš kurios, kai $x>N$, gauname

$$f(x)\geqslant a_n x^{n-m+1}\left(x^{m-1}-\left(\frac{A_1}{a_n}\right)^{(m-1)/m}\right)>$$

$$>a_n x^{n-m+1}\left(\left(\frac{A_1}{a_n}\right)^{(m-1)/m}-\left(\frac{A_1}{a_n}\right)^{(m-1)/m}\right)=0.$$

Pastaroji nelygybė reiškia, kad $f(x)>0$, kai $x>N$. Iš čia išplaukia teoremos teiginys.

Pavyzdys. Polinomo $3x^7+4x^5+5x^4-15x^3-13x^2+11x+10$ teigiamosios šaknys mažesnės už skaičių

$$N=1+\sqrt[4]{\frac{15}{3}}=1+\sqrt[4]{5}.$$

Remdamiesi įrodytomis teoremomis, dažniausiai randame labai netikslų intervalą, kuriame yra realiosios polinomo šaknys. Išnagrinėsime Niutono metodą, kuriuo tą intervalą galėsime rasti norimu tikslumu.

176 teorema. *Jeigu* $f(c)>0$ *ir* $f^{(k)}(c)\geqslant 0$ $(k=1, 2, \ldots, n)$ *su kuriuo nors* $c>0$, *tai, kad ir koks būtų* $l\geqslant c$, *polinomo* $f(x)$ *reikšmė taške* l *yra teigiama.*

Įrodymas. Pasinaudoję Teiloro formule

$$f(x)=f(c)+\sum_{k=1}^{n}\frac{1}{k!}f^{(k)}(c)(x-l)^k$$

ir teoremos sąlygomis, kai $l\geqslant c$, gauname $f(l)>0$.

Taigi, jeigu polinomo ir jo išvestinių reikšmės kuriame nors taške $c>0$ yra teigiamos, tai polinomas neturi teigiamų šaknų, didesnių už c. Todėl polinomo $f(x)$ teigiamų šaknų viršutinis rėžis yra kiekvienas teigiamasis skaičius c, tenkinantis teoremos sąlygas.

Pavyzdys. Polinomo $f(x)=3x^7+4x^6+5x^4-15x^3-13x^2+11x+10$ ir jo išvestinių

$$f^{(1)}(x)=21x^6+20x^4+20x^3-45x^2-26x+11,$$
$$f^{(2)}(x)=3\cdot 7\cdot 6x^5+80x^3+60x^2-90x-26,$$
$$f^{(3)}(x)=3\cdot 7\cdot 6\cdot 5x^4+240x^2-120x-90,$$
$$f^{(4)}(x)=3\cdot 7\cdot 6\cdot 5\cdot 4x^3+480x+120,$$
$$f^{(5)}(x)=3\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3x^2+480,$$
$$f^{(6)}(x)=3\cdot 7!\,x,$$
$$f^{(7)}(x)=3\cdot 7!$$

reikšmės yra teigiamos taške $x=1$. Todėl tas polinomas neturi teigiamų šaknų, didesnių už 1. Kaip matome, teigiamųjų šaknų viršutinis rėžis 1 daugiau kaip du kartus mažesnis už $N=1+\sqrt[4]{5}$.

Remdamiesi 176 arba 175 teorema, galime rasti teigiamų šaknų apatinį rėžį, neigiamų šaknų viršutinį bei apatinį rėžius.

Norėdami rasti polinomo $f(x)$, kurio $a_0\neq 0$, teigiamų šaknų apatinį rėžį, atliekame keitinį $x=\frac{1}{y}$. Jeigu $\deg(f)=n$, tai žymime $f\left(\frac{1}{y}\right)=\frac{1}{y^n}f_1(y)$. Polinomo $f_1(y)$ teigiamų šaknų viršutinį rėžį c_1 randame išdėstytu metodu, t. y. imame tokį c_1, kad $f_1(c_1)>0$ ir $f_1^{(k)}(c_1)\geqslant 0$, $k=1, 2, \ldots, n$. Kadangi polinomo $f(x)$ ir $f_1(y)$ šaknys susietos lygybe $x=\frac{1}{y}$, tai $c=\frac{1}{c_1}$ yra polinomo $f(x)$ teigiamų šaknų apatinis rėžis.

Norėdami rasti polinomo $f(x)$ neigiamų šaknų apatinį rėžį, atliekame keitinį $x=-y$. Jeigu polinomo $f(-y)=f_2(y)$ teigiamų šaknų viršutinis rėžis yra d, tai polinomo $f(x)$ neigiamų šaknų apatinis rėžis yra $-d$, nes polinomų $f(x)$ ir $f_2(y)$ šaknys susietos lygybe $x=-y$. Ieškodami polinomo $f(x)$ neigiamų šaknų viršutinio rėžio, atliekame keitinį $x=-\frac{1}{y}$. Randame polino-

mo $f_3(y)$, $f\left(-\frac{1}{y}\right)=\frac{1}{y^n}f_3(y)$, teigiamų šaknų viršutinį rėžį b. Kadangi polinomų $f(x)$ ir $f_3(y)$ šaknys susietos lygybe $x=-\frac{1}{y}$, tai polinomo $f(x)$ neigiamų šaknų viršutinis rėžis yra $-\frac{1}{b}$.

Taigi kiekvienam nenulinio laipsnio polinomui su realiaisiais koeficientais galime rasti du tokius intervalus $[-M_1, -m_1]$ ir $[m, M]$, už kurių nėra polinomo $f(x)$ realiųjų šaknų. Pateiktasis metodas vadinamas Niutono metodu.

Pavyzdys. Rasime polinomo $f(x)=x^5-3x^3+4x-10$ teigiamų šaknų viršutinį rėžį ir neigiamų šaknų apatinį rėžį.

Apskaičiuojame išvestines

$$f^{(1)}(x)=5x^4-9x^2+4,$$
$$f^{(2)}(x)=20x^3-18x,$$
$$f^{(3)}(x)=60x^2-18,$$
$$f^{(4)}(x)=120x,$$
$$f^{(5)}(x)=120.$$

Randame kiek galima mažesnį nelygybių sistemos

$$f(x)>0,\ f^{(k)}(x)\geqslant 0,\quad k=1,\ \ldots,\ 5,$$

teigiamą sprendinį, pavyzdžiui 2. Tai ir yra teigiamų šaknų viršutinis rėžis. (Aišku, jis nėra labai tikslus, bet jo tikslinimas susijęs su dideliais skaičiavimais.)

Rasime neigiamų šaknų apatinį rėžį. Pakeitę $x=-y$, gauname polinomą $f(x)=f(-y)=-y^5+3y^2-4y-10$, t. y.

$$f_2(y)=y^5-3y^2+4y+10.$$

Jo išvestinių

$$f_2^{(1)}(y)=5y^4-9y^2+4,$$
$$f_2^{(2)}(y)=20y^3-18y,$$
$$f_2^{(3)}(y)=60y^2-18,$$
$$f_2^{(4)}(y)=120y,$$
$$f_2^{(5)}(y)=120$$

reikšmės, kaip ir paties polinomo reikšmė, yra teigiamos taške 2. Todėl -2 yra polinomo $f(x)$ neigiamų šaknų apatinis rėžis. Taigi polinomas $f(x)$ intervalo $[-2, 2]$ išorėje neturi realiųjų šaknų. Atkreipsime dėmesį į tai, kad pagal 174 teoremą gauname intervalą $[-11, 11]$, o pagal 175 teoremą – intervalą $[-(1+\sqrt{10}), 1+\sqrt{10}]$, t. y. gauname žymiai didesnius intervalus.

Uždaviniai

7. Raskite intervalą, kuriame yra polinomo $f(x)$ visos realiosios šaknys:

a) $f(x)=5x^6-4x^5+7x^4-3x^3-6x^2+4x-5$;

b) $f(x)=4x^7+8x^5+6x^4-7x^3-10x^2+14x-15$.

8. Raskite polinomo $f(x)$ teigiamų šaknų viršutinį ir apatinį rėžius ir neigiamų šaknų viršutinį ir apatinį rėžius:

a) $f(x)=x^4+4x^3-8x^2-10x+14$;

b) $f(x)=x^5+7x^3-3$.

§91. Polinomo virš R realiųjų šaknų skaičiaus nustatymas ir šaknų atskyrimo Šturmo metodas

Polinomo su realiaisiais koeficientais realiųjų šaknų skaičių galima nustatyti keliais metodais. Kai kurie iš jų labai paprasti, bet juos taikant gaunamas netikslus atsakymas. Taigi visų metodų nenagrinėsime, susipažinsime tik su Šturmo metodu (J. CH. F. Sturm, 1803–1855, šveicarų matematikas). Nors tas metodas ir nėra labai paprastas, bet jį taikydami visada gauname tikslų atsakymą.

Jeigu kurio nors intervalo $[a, b]$ galuose polinomo $f(x)$ reikšmės yra skirtingų ženklų, t. y. $f(a)f(b)<0$, tai intervale $[a, b]$ yra ne mažiau kaip viena polinomo $f(x)$ realioji šaknis. Jų gali būti lyginiu skaičiumi daugiau. Tai išplaukia iš polinominės funkcijos tolydumo ir minėtosios Bolcano teoremos. Jeigu $f(a)f(b)>0$, tai iš tų pačių faktų išplaukia, kad intervale $[a, b]$ polinomo realiųjų šaknų skaičius lyginis, t. y. arba visai jų nėra, arba yra 2, 4, ... realiosios šaknys.

Tarkime, kad $f(x)$ yra n-ojo ($n\geqslant 2$) laipsnio polinomas su realiaisiais koeficientais, neturintis kartotinių šaknų, t. y. $\mathrm{D}(f, f')=1$. (Aišku, mūsų samprotavimai teisingi ir kai $n\geqslant 1$. Kai $n=1$, polinomas turi realiąją šaknį. Kai $n=2$, naudojantis kvadratinės lygties sprendimo formulėmis, galima apskaičiuoti polinomo šaknis ir nustatyti, ar jos realios, ar menamos. Taigi dėstomasis metodas taikytinas bent jau tuo atveju, kai $n>2$.)

Sudarysime polinomų seką $f_0(x)=f(x)$, $f_1(x)=f'(x)$, $f_2(x)$, ..., $f_m(x)$ šitokiu būdu:

$$f_{k-2}(x)=f_{k-1}(x)\,q_{k-1}(x)-f_k(x), \quad k=2, \ldots, m.$$

Aiškiai matyti, kad polinomas $f_k(x)$ lygus liekanai, gautai polinomą $f_{k-2}(x)$ padalijus iš polinomo $f_{k-1}(x)$ ir paimtai su priešingu ženklu.

Taigi, žinodami polinomą $f(x)$, galime nuosekliai apskaičiuoti $f_1(x)$, $f_2(x)$, ..., $f_m(x)$. Iš 142 dalybos su liekana teoremos išplaukia, kad tie polinomai apibrėžti vienareikšmiškai, o iš Euklido algoritmo išeina, kad polinomų seka yra baigtinė.

Sudarytoji polinomų seka $f_0(x)=f(x)$, $f_1(x)=f'(x)$, $f_2(x)$, ..., $f_m(x)$ pasižymi šiomis savybėmis.

I savybė. *Jokie du gretimi tos sekos polinomai neturi bendrų šaknų.*

Įrodymas. Kadangi $\mathrm{D}(f, f')=1$, tai $f_0(x)$ ir $f_1(x)$ neturi bendrų šaknų. Tarkime, kad $f_{k-1}(x)$ ir $f_k(x)$ neturi bendrų šaknų. Jeigu $f_{k+1}(x)$ ir $f_k(x)$ turi bendrą šaknį l, tai iš lygybės

$$f_{k-1}(x)=f_k(x)\,q_k(x)-f_{k+1}(x)$$

išplaukia, kad l yra ir polinomo $f_{k-1}(x)$ šaknis, t. y. $f_{k-1}(x)$ ir $f_k(x)$ turi bendrą šaknį l. Tai prieštarauja prielaidai. Todėl $f_{k+1}(x)$ ir $f_k(x)$ bendrų šaknų neturi. Imdami iš eilės $k=1, \ldots, m-1$, įrodome savybę.

II savybė. *Jeigu l yra polinomo $f_k(x)$ šaknis, tai $f_{k-1}(l)$ ir $f_{k+1}(l)$ yra skirtingų ženklų* $(k=1, \ldots, m-1)$.

Įrodymas. Į išraišką

$$f_{k-1}(x)=f_k(x)\,q_k(x)-f_{k+1}(x)$$

įrašę $x=l$ ir pasinaudoję lygybe $f_k(l)=0$, gauname

$$f_{k-1}(l)=-f_{k+1}(l).$$

III savybė. *Jeigu l yra polinomo $f(x)$ šaknis, tai su pakankamai mažu $\varepsilon>0$ teisingos nelygybės $f_0(l-\varepsilon)f_1(l-\varepsilon)<0$ ir $f_0(l+\varepsilon)f_1(l+\varepsilon)>0$.*

Įrodymas. Kadangi polinomas $f(x)$ neturi kartotinių šaknų, o $f(l)=0$, tai, esant pakankamai mažam $\varepsilon>0$, galimi du atvejai: a) $f(l-\varepsilon)<0$ ir $f(l+\varepsilon)>0$, b) $f(l-\varepsilon)>0$ ir $f(l+\varepsilon)<0$. Pirmuoju atveju funkcijos $f(x)$ reikšmės intervale $[l-\varepsilon, l+\varepsilon]$ didėja, todėl jos išvestinė $f_1(x)=f'(x)$ visame intervale teigiama, t. y. $f_1(l-\varepsilon)>0$ ir $f_1(l+\varepsilon)>0$. Antruoju atveju funkcijos $f(x)$ reikšmės intervale $[l-\varepsilon, l+\varepsilon]$ mažėja, taigi jos išvestinė visame intervale neigiama, t. y. $f_1(l-\varepsilon)<0$ ir $f_1(l+\varepsilon)>0$. Todėl abiem atvejais

$$f(l-\varepsilon)f_1(l-\varepsilon)<0, \quad f(l+\varepsilon)f_1(l+\varepsilon)>0.$$

IV savybė. *Polinomas $f_m(x)$ neturi realiųjų šaknų.*

Kadangi iš Euklido algoritmo gauname $\mathbf{D}(f,f')=cf_m(x)$, o $\mathbf{D}(f,f')=1$, tai $f_m(x)=a$ yra skaičius.

Sudarytąją polinomų seką, taip pat kiekvieną kitą polinomų seką $f_0(x)=f(x), f_1(x)=cf'(x), \varphi_2(x), \ldots, \varphi_r(x)$, $c>0$, pasižyminčią I–IV savybėmis, vadiname polinomo $f(x)$ Šturmo grandine.

Pavyzdys. Polinomo $f(x)=x^4-4x^3+4x^2-4$ Šturmo grandinė yra šitokia:

$$f_0(x)=f(x),$$

$$\varphi_1(x)=\frac{1}{4}f'(x)=x^3-3x^2+2x,$$

$$\varphi_2(x)=x^2-2x+4,$$

$$\varphi_3(x)=x-1,$$

$$\varphi_4(x)=-1.$$

Kad suprastute, kaip reikia naudotis Šturmo grandine realiųjų šaknų skaičiui nustatyti, išaiškinsime, ką reiškia *ženklo pokyčių skaičius sekoje ir ženklo pokyčių nuostolis intervale.*

Šturmo grandinės polinomuose vietoje x įrašę realųjį skaičių a, gauname skaičių seką

$$f_0(a), f_1(a), f_2(a), \ldots, f_m(a),$$

kurioje gali būti teigiamų, neigiamų ir lygių nuliui skaičių. Vietoje skaičių įrašę jų ženklus, nuliui nepriskirdami jokio ženklo, gauname ženklų +, − seką, kurios ženklo pokyčių skaičių žymėsime $I(a)$. Pavyzdžiui, seką

$$1,\ 3,\ -4,\ 0,\ -5,\ 1,\ 3$$

atitinka ženklų seka +, +, −, ,−, +, +, kurioje yra 2 ženklo pokyčiai: iš + į − ir iš −į +, t. y. $I=2$.

Paėmę kitą realųjį skaičių b $(a<b)$, gauname kitą skaičių seką

$$f_0(b),\ f_1(b),\ f_2(b),\ \ldots,\ f_m(b),$$

kurią atitinka jos ženklų seka, turinti savo ženklo pokyčių skaičių $I(b)$.

Skirtumas $I(a)-I(b)$ *vadinamas Šturmo grandinės ženklo pokyčių nuostoliu intervale* $[a,\ b]$.

177 (Šturmo) teorema. *Jeigu polinomas* $f(x)$ *neturi kartotinių šaknų ir* $f(a)\neq 0$, $f(b)\neq 0$, $a<b$, *tai jo realiųjų šaknų skaičius intervale* $[a,\ b]$ *lygus jo Šturmo grandinės ženklo pokyčių nuostoliui tame intervale.*

Įrodymas. Tarkime, kad x didėja nuo a iki b. Išnagrinėsime, kaip kinta ženklo pokyčių skaičius Šturmo grandinėje

$$f_0(x),\ f_1(x),\ f_2(x),\ \ldots,\ f_m(x).$$

Jeigu $x=l$ yra polinomo $f_k(x)$, $k=1,\ \ldots,\ m-1$, šaknis, tai iš I savybės išplaukia, kad $f_{k-1}(l)\neq 0$, $f_{k+1}(l)\neq 0$ ir $f_{k-1}(l)=-f_{k+1}(l)$. Sakykime, $\varepsilon>0$ toks mažas, kad intervale $[l-\varepsilon,\ l+\varepsilon]$ polinomai $f_{k-1}(x)$ ir $f_{k+1}(x)$ neturi šaknų (tokį ε galima rasti, nes funkcijos $f_{k-1}(x)$ ir $f_{k+1}(x)$ yra tolydžios). Sekos $f_{k-1}(x)$, $f_k(x)$, $f_{k+1}(x)$ galimus ženklus intervale $[l-\varepsilon,\ l+\varepsilon]$ pateiksime lentelėje.

x	$f_{k-1}(x)$	$f_k(x)$	$f_{k+1}(x)$	I
$l-\varepsilon\leqslant x<l$	−	$\begin{matrix}-\\+\end{matrix}$	+	1
$l<x\leqslant l+\varepsilon$	−	$\begin{matrix}+\\-\end{matrix}$	+	1
$l-\varepsilon\leqslant x<l$	+	$\begin{matrix}-\\+\end{matrix}$	−	1
$l<x\leqslant l+\varepsilon$	+	$\begin{matrix}+\\-\end{matrix}$	−	1

Matome, kad ženklo pokyčių skaičius yra tas pats, t. y. lygus vienetui. Kadangi pagal I savybę jokie du gretimi polinomai neturi lygių šaknų, tai, kai x didėdamas pereina per polinomo $f_k(x)$, $k=1,\ \ldots,\ m-1$, šaknį, Šturmo grandinėje ženklo pokyčių skaičius lieka toks pat.

Jeigu $x=l$ yra polinomo $f(x)$ šaknis, tai pagal III savybę nustatome tokį sekos $f_0(x)$, $f_1(x)$ ženklo pokyčių skaičių intervale $[l-\varepsilon,\ l+\varepsilon]$ (jame $f(x)$ neturi kitų šaknų):

x	$f_0(x)$	$f_1(x)$	I
$l-\varepsilon \leqslant x < l$	−	+	1
$l < x \leqslant l+\varepsilon$	+	+	0
$l-\varepsilon \leqslant x < l$	+	−	1
$l < x \leqslant l+\varepsilon$	−	−	0

Taigi, kai x didėdamas pereina per polinomo $f(x)$ šaknį, Šturmo grandinės ženklo pokyčių nuostolis lygus vienetui. Kadangi paskutinis Šturmo grandinės polinomas neturi realiųjų šaknų, t. y. jo reikšmės yra to paties ženklo, tai Šturmo grandinės ženklo pokyčių nuostolis intervale $[a, b]$ lygus polinomo $f(x)$ realiųjų šaknų skaičiui intervale $[a, b]$.

Pavyzdys. Nustatysime polinomo $x^4-4x^3+4x^2-4$ realiųjų šaknų skaičių. To polinomo Šturmo grandinė yra $f_0(x)=f(x)$, $f_1(x)=x^3-3x^2+2x$, $f_2(x)=x^2-2x+4$, $f_3(x)=x-1$, $f_4(x)=-1$. Sudarome ženklų lentelę ir nustatome ženklo pokyčių skaičių bei ženklo pokyčių nuostolį intervaluose $(-\infty,\ \infty)$, $[-1,\ 0]$, $[2,\ 3]$.

x	$f(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	I	
$-\infty$	+	−	+	−	−	3	}
−1	+	−	+	−	−	3	}
0	−		+	−	−	2	}
2	−	+	+	+	−	2	}
3	+	+	+	+	-	1	
$+\infty$	+	+	+	+	−	1	

Matome, kad intervale $(-\infty,\ \infty)$ Šturmo grandinės ženklo pokyčių nuostolis lygus 2. Taigi polinomas turi dvi realiąsias šaknis, kurios yra intervaluose $[-1,\ 0]$ ir $[2,\ 3]$ — tai matyti lentelėje.

Remdamiesi Šturmo teorema, galime nustatyti, kiek iš viso realiųjų šaknų turi polinomas $f(x)$ su realiaisiais koeficientais. Pakanka apskaičiuoti, kam lygus jo Šturmo grandinės ženklo pokyčių nuostolis intervale $(-\infty, \infty)$. Be to, galime ir atskirti realiąsias šaknis vieną nuo kitos, t. y. nustatyti intervalus, kuriuose būtų po vieną realiąją šaknį. Užtenka rasti tokius intervalus (paprastai vienetinio ilgio arba trumpesnius), kuriuose Šturmo grandinės ženklo pokyčių nuostolis lygus vienetui. Tokie intervalai dažniausiai randami bandymu.

Atskirti polinomo $f(x)$ realiąsias šaknis vieną nuo kitos labai svarbu tada, kai norime vieną ar kelias realiąsias šaknis apskaičiuoti nurodytu tikslumu. Visi apytikslio realiųjų šaknų skaičiavimo metodai paremti tuo, kad, prieš pradedant juos taikyti, turi būti žinomas intervalas, kuriame yra tik ieškomoji šaknis.

Uždaviniai

9. Sudarykite polinomo $f(x)$ Šturmo grandinę, nustatykite realiųjų šaknų skaičių ir atskirkite jas, kai:

a) $f(x)=x^3-6x^2+9x-3$;

b) $f(x)=x^4-4x^3+6x^2-5x+1$;

c) $f(x)=x^4+3x^3+4x^2+2x-1$.

§92. Polinomo su realiaisiais koeficientais realiųjų šaknų skaičiavimo artutiniai metodai

Nagrinėsime polinomą $f(x)$ su realiaisiais koeficientais, neturintį kartotinių šaknų. Tarkime, kad intervale $[a, b]$ yra tik viena to polinomo šaknis α, kurią reikia apskaičiuoti nurodytu tikslumu $\delta>0$, t. y. reikia rasti tokį skaičių l, kad būtų $|l-\alpha|\leqslant\delta$.

Kiekvienas artutinis metodas yra algoritmas, kuriuo galime sukonstruoti tokią racionaliųjų skaičių seką $l_1, l_2, \ldots, l_m, \ldots$, kurios riba lygi α, ir su kiekvienu $m\in\mathbf{N}$ nustatyti, už kokį skaičių ne didesnis skirtumas $|l_m-\alpha|$.

Norėdami apskaičiuoti šaknį nurodytu tikslumu δ, turime rasti tokį sekos $\{l_j\}$ narį l_m, kad būtų $|l_m-\alpha|\leqslant\delta$. Naudodamiesi algoritmu, sekos narius $l_1, l_2, \ldots, l_m, \ldots$ galime apskaičiuoti tik nuosekliai, vieną po kito. *Narį l_k vadinsime k-uoju artiniu.*

Nėra paprasta palyginti du metodus ir nustatyti, kuris iš jų efektyvesnis. Reikia atsižvelgti į konvergavimo greitį ir į tai, kiek veiksmų reikia atlikti skaičiuojant eilinį artinį l_k.

1. Intervalo dalijimo pusiau metodas. Jeigu žinome, kad intervale $[a, b]$ yra tik viena polinomo $f(x)$ šaknis α, tai $f(a)f(b)<0$, t. y. intervalo galuose polinomo reikšmės yra skirtingų ženklų. Intervalą $[a, b]$ dalijame pusiau ir gauname intervalus $\left[a, \frac{a+b}{2}\right], \left[\frac{a+b}{2}, b\right]$. Jeigu $f\left(\frac{a+b}{2}\right)\neq 0$, tai iš gautųjų

intervalų imame tą, kurio galuose polinomo reikšmės yra skirtingų ženklų, ir žymime $[a_1, b_1]$. Tą procesą tęsiame toliau. Gautąjį intervalą $[a_j, b_j]$ dalijame pusiau ir $[a_{j+1}, b_{j+1}]$ žymime tą intervalą iš $\left[a_j, \frac{a_j+b_j}{2}\right]$, $\left[\frac{a_j+b_j}{2}, b_j\right]$, kurio galuose polinomo reikšmės yra skirtingų ženklų. Tuo būdu gauname intervalų seką $[a, b]$, $[a_1, b_1]$, ..., $[a_j, b_j]$, ... Kiekviename iš jų yra polinomo šaknis. Be to, $b_j-a_j=\frac{1}{2}(b_{j-1}-a_{j-1})=\ldots=\frac{1}{2^j}(b-a)$. Pažymėję $l_j=\frac{1}{2}(a_j+b_j)$, gausime seką $\{l_j\}$, kurios riba $\lim\limits_{j\to\infty} l_j=\alpha$, be to, $|l_j-\alpha|\leqslant$ $\leqslant\frac{1}{2^{j+1}}(b-a)$.

Taigi, norint apskaičiuoti šaknį α tikslumu δ, reikia imti artinį l_m su mažiausiu numeriu m, tenkinančiu nelygybę

$$\frac{1}{2^{m+1}}(b-a)\leqslant\delta,$$

t. y.

$$m\geqslant\frac{\lg(b-a)-\lg\delta}{\lg 2}-1.$$

Pavyzdys. Norint rasti polinomo $f(x)$ šaknį 0,01 tikslumu, kai $b-a=1$, užtenka parinkti $m\geqslant\frac{2}{\lg 2}-1$, t. y. $m=6$. Taigi tuo atveju šešis atitinkamus intervalus reikia dalyti pusiau ir imti $l_m=l_6=\frac{a_6+b_6}{2}$. Paklaida bus ne didesnė už $\frac{1}{128}<0{,}01$. Norint rasti šaknį 0,001 tikslumu, užtenka imti $l_9=\frac{a_9+b_9}{2}$. Paklaida bus ne didesnė už $\frac{1}{1024}<0{,}001$.

Taikant tą metodą, skaičiavimo procesas labai paprastas – tereikia nustatyti polinomo reikšmių $f\left(\frac{a_j+b_j}{2}\right)$ ženklus ($j=0, 1, 2, \ldots$), tačiau techniškai sunkiai realizuojamas. Kai n dideli (pvz. $n\geqslant 5$), jau skaičiuojant artinius su nedideliais numeriais, tenka operuoti dideliais skaičiais (trupmenomis su dideliais vardikliais), o konvergavimo greitis mažas.

Pavyzdys. Apskaičiuosime polinomo

$$f(x)=x^4-4x^3+4x^2-4$$

mažiausią realiąją šaknį 0,1 tikslumu. Aišku, reikia rasti l_3, nes $|l_3-\alpha|\leqslant\frac{1}{16}<0{,}1$.

Esame nustatę (žr. § 91), kad to polinomo mažiausioji šaknis yra intervale $[-1, 0]$, be to, $f(-1)>0$, $f(0)<0$. Apskaičiavę gauname $f\left(-\frac{1}{2}\right)=\frac{-39}{16}<0$. Todėl šaknis yra intervale $\left[-1, -\frac{1}{2}\right]$. Vėl apskaičiuojame $f\left(-\frac{3}{4}\right)=\frac{65}{256}>0$, taigi šaknis yra intervale $\left[-\frac{3}{4}, -\frac{1}{2}\right]$. Apskaičiavę gauname $f\left(-\frac{5}{8}\right)<0$, todėl šaknis yra intervale $\left[-\frac{3}{4}, -\frac{5}{8}\right]$.

Laikydami $\alpha\approx-\frac{11}{16}$, padarysime paklaidą, ne didesnę už $\frac{1}{16}$.

2. Lagranžo metodas. Taikant šį metodą, *nuosekliai apskaičiuojami šaknies skleidimo grandinine trupmena* $\alpha=[q_0, q_1, q_2, \ldots]$ *elementai* $q_0, q_1, \ldots$ *ir apytiksle šaknies reikšme laikomas atitinkamos eilės reduktas.* Paklaida skaičiuojama remiantis 39 teorema.

Tarkime, kad tik viena polinomo $f(x)$ šaknis α yra intervale $[q_0, q_0+1]$, q_0 – sveikasis skaičius. Tada $\alpha=q_0+\alpha_1, 0<\alpha_1<1$. Žymime $\alpha_1=\frac{1}{y}$ ir keitiniu $x=q_0+\frac{1}{y}$ iš lygties $f(x)=0$ gauname lygtį $f_1(y)=0, f_1(y)$ turi didesnę už 1 šaknį. (Jeigu lygtis $f(x)=0$ intervale $[q_0, q_0+1]$ turėtų daugiau kaip vieną šaknį, tai polinomas $f_1(y)$ turėtų tiek pat didesnių už vienetą šaknų. Todėl reikėtų išrinkti vieną iš jų).

Polinomo $f_1(y)$ didesnę už vienetą šaknį, atitinkančią polinomo $f(x)$ šaknį α, pažymėję y_1, gauname lygybę

$$\alpha=q_0+\frac{1}{y_1}.$$

Tarkime, kad $q_1<y_1<q_1+1$, q_1 – natūrinis skaičius. Tą skaičių galime rasti, pavyzdžiui, Šturmo metodu arba tiesiogiai tikrindami.

Vėl keitiniu $y=q_1+\frac{1}{z}$ iš lygties $f_1(y)=0$ gauname lygtį

$$f_2(z)=0.$$

$f_2(z)$ turi didesnę už vienetą šaknį. Randame intervalą $[q_2, q_2+1]$, kuriame yra šaknį y_1 atitinkanti šaknis z_1. Procesą tęsiame toliau. Po k žingsnių gauname

$$\alpha=q_0+\frac{1}{y_1}=q_0+\frac{1}{q_1+\frac{1}{z_2}}=\ldots=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{}{\cdots\cdots+\cfrac{1}{q_k+\frac{1}{w_k}}}}}.$$

Paėmę $l_k=[q_0, q_1, \ldots, q_k]$, $k=0, 1, \ldots$, gauname racionaliųjų skaičių $l_k=\frac{P_k}{Q_k}$ (žr. § 21) seką, kurios riba yra skaičius α, t. y. polinomo $f(x)$ šaknis. Remdamiesi 31 ir 39 teoremomis, apskaičiuojame paklaidą ir gauname

$$|l_k-\alpha|\leqslant\frac{1}{Q_k(Q_k+Q_{k-1})};$$

čia Q_i, $i=k-1, k$, – i-ojo redukto vardiklis.

Norėdami apskaičiuoti α tikslumu δ, turime imti artinį l_m su mažiausiu natūriniu numeriu m, su kuriuo teisinga nelygybė

$$\frac{1}{Q_m(Q_m+Q_{m-1})}\leqslant\delta,$$

t. y. $Q_m(Q_m+Q_{m-1})\geqslant\frac{1}{\delta}$.

Pavyzdys. Rasime polinomo $f(x)=x^4-4x^3+4x^2-4$ šaknį, kuri yra intervale [2, 3], 0,01 tikslumu.

Turime $q_0=2$. Atlikę keitinį $x=2+\frac{1}{y}$, gauname

$$f(x)=\frac{1}{y^4}(4y^4-4y^2-4y-1).$$

Polinomas $f_1(y)=4y^4-4y^2-4y-1$ turi teigiamą šaknį intervale [1, 2], todėl $q_1=1$.

Atlikę keitinį $y=1+\frac{1}{z}$, gauname

$$f_1(y)=-\frac{1}{z^4}(5z^4-4z^3-20z^2-16z-4).$$

Polinomas $f_2(z)=5z^4-4z^3-20z^2-16z-4$ turi teigiamą šaknį intervale [2, 3], taigi $q_2=2$.

Pažymėję $z=2+\frac{1}{v}$, gauname polinomą

$$f_3(v)=68v^4-16v^3-76v^2-46v-5,$$

kuris turi didesnę už vienetą šaknį intervale [1, 2]. Taigi $q_3=1$.

Po keitinio $v=1+\frac{1}{u}$ gauname polinomą

$$f_4(u)=65u^4-36x^3-284u^2-256u-68,$$

kurio teigiama šaknis yra intervale [2, 3], t. y. $q_4=2$.

Gauname apytiksles šaknies reikšmes

$$l_0=2,\ l_1=[2,\ 1]=3,\ l_2=[2,\ 1,\ 2]=\frac{8}{3},\ l_3=[2,\ 1,\ 2,\ 1]=\frac{11}{4},\ l_4=[2,\ 1,\ 2,\ 1,\ 2]=\frac{30}{11}.$$

Paėmę $\alpha\approx l_4$, įvertiname paklaidą

$$|l_4-\alpha|\leqslant\frac{1}{Q_4(Q_4+Q_3)}=\frac{1}{11\cdot 15}<0{,}01.$$

Tuo atveju, *kai ieškomoji polinomo šaknis* α *intervale* $[q_0,\ q_0+1]$ *yra racionalusis skaičius, ją galima rasti Lagranžo metodu (jei rasime pakankamą reduktų skaičių), nes racionalusis skaičius išskleidžiamas baigtine grandinine trupmena.*

Jeigu intervale $[q_0,\ q_0+1]$ yra šaknys $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_s$ $(\alpha_1<\alpha_2<\ldots<\alpha_s)$, tai tas šaknis atitinka didesnės už vienetą polinomo $f_1(y)$ šaknys mažėjimo tvarka, t. y. $y_1>y_2>\ldots>y_s$, nes

$$q_0+\frac{1}{y_i}<q_0+\frac{1}{y_j}$$

tada, kai $y_i>y_j$.

Todėl, ieškant eilinio vardiklio q_1, reikia į tai atsižvelgti. Taip pat reikia prisiminti, kad skirtingos šaknys $y_1,\ \ldots,\ y_s$ gali turėti lygias sveikąsias dalis. Tada ir toliau reikės analogiškai samprotauti.

Skaičiavimai, kuriuos reikia atlikti ieškant šaknies artinių Lagranžo metodu, paprasti. Tai polinomo skleidimas dvinario laipsniais ir polinomo reikšmės ženklo nustatymas taškuose $l\in\mathbf{N}$, ieškant intervalo $[q_j,\ q_j+1]$, kuriame yra eilinio polinomo šaknis. Artėjimo greitis iš esmės priklauso nuo grandininės trupmenos elementų q_j, $j=1,\ 2,\ \ldots$ Jis bus didelis, kai $q_1,\ q_2\ \ldots$ dideli skaičiai, ir mažas, kai $q_1,\ q_2,\ \ldots$ artimi 1.

3. Hornerio metodas. Tarkime, kad polinomo $f(x)$ realioji šaknis išreikšta dešimtaine begaline trupmena

$$\alpha = c_0 + \sum_{j=1}^{\infty} \frac{c_j}{10^j};$$

čia c_0 – sveikasis skaičius, o c_1, c_2, c_3, ... – sveikieji neneigiami skaičiai, ne didesni už 9.

Skaičių c_0 randame tikrindami arba atskirdami šaknis Šturmo metodu. Nustatome, kad intervale $[c_0, c_0+b]$, $0<b\leqslant 1$, yra tik viena šaknis. Keitiniu $x-c_0=y$ iš polinomo $f(x)$ gauname polinomą $f_1(y)$, kurio koeficientai lygūs $f(x)$ skleidinio $x-c_0$ laipsniais pagal Teiloro formulę koeficientams. Polinomas $f_1(y)$ turi šaknį $y=\alpha-c_0=0,c_1c_2\ldots$ Atlikę dar vieną keitinį

$$y=\frac{z}{10},$$

gauname polinomą $\varphi_1(z)$:

$$f_1(y)=f_1\left(\frac{z}{10}\right)=\frac{1}{10^n}\,\varphi_1(z)$$

(čia $n=\deg(f)$), kurio šaknis yra

$$x_1=c_1,c_2c_3\ldots$$

Tos šaknies sveikąją dalį c_1, $0\leqslant c_1\leqslant 9$, randame kuriuo nors būdu, pavyzdžiui, tikrindami.

Tokiu būdu radę polinomo $\varphi_k(z)$ šaknies sveikąją dalį c_k, $k=1, 2, \ldots$, keitiniu $z-c_k=u$ gauname polinomą $f_{k+1}(u)$, kurio koeficientai yra polinomo $f_k(z)$ skleidinio dvinario $z-c_k$ laipsniais pagal Teiloro formulę koeficientai. Po to keitiniu

$$u=\frac{v}{10}$$

gauname polinomą $\varphi_{k+1}(v)$,

$$f_{k+1}(u)=f_{k+1}\left(\frac{v}{10}\right)=\frac{1}{10^n}\varphi_{k+1}(v),$$

kurio šaknis yra $c_{k+1}, c_{k+2}c_{k+3}\ldots$

Tos šaknies sveikąją dalį c_{k+1}, $0\leqslant c_{k+1}\leqslant 9$, randame kuriuo nors būdu.

Polinomo φ_{k+1} koeficientus b_j gauname iš polinomo f_{k+1} koeficientų a_j, $k=0, 1, \ldots$, padauginę juos iš 10^{n-j}, $j=0,1, \ldots, n$, $n=\deg(f)$.

Kadangi

$$\alpha=c_0+\frac{x_1}{10},$$

$$x_1=c_1+\frac{x_2}{10},$$

$$\ldots\ldots\ldots$$

$$x_k=c_k+\frac{x_{k+1}}{10},$$

tai

$$\alpha = c_0 + \frac{c_1}{10} + \frac{c_2}{10^2} + \ldots + \frac{c_k}{10^k} + \frac{x_{k+1}}{10^{k+1}}.$$

Paėmę

$$l_m = c_0 + \sum_{j=1}^{m} c_j 10^{-j},$$

gauname seką $l_1, l_2, \ldots, l_m, \ldots$, kurios $\lim\limits_{m\to\infty} l_m = \alpha$. Be to,

$$|l_m - \alpha| \leqslant 10^{-m},$$

nes $0 \leqslant x_{m+1} < 10$. Tai reiškia, kad l_m yra šaknies α apytikslė reikšmė 10^{-m} tikslumu.

Išnagrinėtasis metodas gana paprastas, greitai gaunamas reikiamas tikslumas, tačiau, praktiškai skaičiuojant, labai greitai auga polinomų φ_k koeficientai. Todėl žymiai sunkiau nustatoma eilinio polinomo šaknies, esančios tarp 0 ir 10, sveikoji dalis.

Pavyzdys. Apskaičiuosime polinomo

$$f(x) = x^5 + 5x^4 + 5x^2 - 15x - 5$$

realiąją šaknį, esančią intervale [1, 2], 0,01 tikslumu.

Aišku, kad $c_0 = 1$.

Norėdami rasti c_1, atliekame keitinį $x - 1 = y$, po to $y = \frac{z}{10}$. Pirmiausia išskleidžiame polinomą $f(x)$ dvinario $x-1$ laipsniais. Naudojamės Hornerio schema:

	1	5	0	5	−15	−5
1	1	6	6	11	−4	−9
1	1	7	13	24	20	
1	1	8	21	45		
1	1	9	30			
1	1	10				
1	1					

Gauname skleidinį

$$f(x) = (x-1)^5 + 10(x-1)^4 + 30(x-1)^3 + 45(x-1)^2 + 20(x-1) - 9.$$

Taigi

$$f_1(y)=y^5+10y^4+30y^3+45y^2+20y-9=\frac{z^5}{10^5}+\frac{z^4}{10^3}+\frac{3z^3}{10^2}+\frac{45z^2}{10^2}+2z-9,$$

todėl

$$\varphi_1(z)=z^5+100z^4+3000z^3+45\,000z^2+200\,000z-900\,000.$$

Randame jo šaknies, esančios tarp 0 ir 10, sveikąją dalį. Ją rasti nėra paprasta, nes koeficientai dideli skaičiai. Kadangi tik paskutinis koeficientas neigiamas, tai gauname $\varphi_1(2)<0$, $\varphi_1(3)>0$. Taigi $c_1=2$.

Po keitinio $z-2=u$ naudojamės Hornerio schema:

	1	1000	3000	45 000	200 000	−900 000
2	1	102	3204	51 408	302 816	−294 368
2	1	104	3412	58 232	419 270	
2	1	106	3624	65 480		
2	1	108	3840			
2	1	110				
2	1					

Taigi

$$f_2(u)=u^5+110u^4+3840u^3+65480u^2+419270u-294368$$

ir

$$\varphi_2(v)=v^5+1100v^4+384\cdot 10^3v^3+6548\cdot 10^4v^2+41927\cdot 10^5v-294368\cdot 10^5.$$

To polinomo šaknis yra tarp 6 ir 7, nes $\varphi_2(6)<0$, o $\varphi_2(7)>0$. Todėl $c_2=6$.

Gavome tokias apytiksles šaknies reikšmes:

$$l_0=1;\ l_1=1{,}2;\ l_2=1{,}26.$$

Taigi 1,26 ir yra apytikslė šaknies reikšmė 0,01 tikslumu. Kitą skaitmenį po kablelio būtų dar sudėtingiau rasti.

Tuo atveju, kai $c_0\geqslant 0$, apytikslę šaknies reikšmę gauname prie c_0 po kablelio prirašę skaitmenis c_1, c_2, ..., c_m, t. y.

$$\alpha\approx l_m=c_0,\overline{c_1c_2\ldots c_m}.$$

Jeigu $c_0<0$, tai

$$l_m=c_0+0,\overline{c_1c_2\ldots c_m},$$

t. y. l_m gaunama prie neigiamojo skaičiaus c_0 pridėjus teigiamąjį skaičių $0,\overline{c_1c_2\ldots c_m}$

Uždaviniai

10. Polinomo $f(x)$ realiąsias šaknis apskaičiuokite Lagranžo metodu 0,001 tikslumu, kai:

a) $f(x)=x^4+x^2-1$;

b) $f(x)=x^4-x^3-2x+1$.

11. Polinomo $f(x)$ realiąsias šaknis apskaičiuokite Hornerio metodu 0,001 tikslumu, kai:

a) $f(x)=x^3-3x-5$;

b) $f(x)=x^4-10x^3+37x^2-58x+31$;

c) $f(x)=x^4+6x^3+15x^2+18x+7$.

Laukų plėtiniai

§93. Transcendentiniai ir algebriniai lauko plėtiniai

Pirmosios dalies 32 paragrafe buvo įvesta lauko plėtinio sąvoka, o 40 paragrafe, nagrinėjant kompleksinius skaičius, buvo suformuluota lauko minimaliojo plėtinio sąvoka. Viena iš priežasčių, dėl kurios gali tekti praplėsti lauką $\mathbf{L}$, yra ta, kad jame gali neturėti šaknies polinomas $f(x) \in L[x]$ (kai $\mathbf{L}$ nėra algebriškai uždaras laukas). Su tokia situacija jau susidūrėme įrodinėdami teoremą apie polinomo šaknies egzistavimą (žr. § 76). Antra vertus, nagrinėdam vieno arba kelių kintamųjų polinomus virš lauko $\mathbf{L}$, gauname jo plėtinius – polinomų virš $\mathbf{L}$ žiedus – integralumo sritis. Jose negalima dalyba. Todėl savo ruožtu tenka spręsti jų praplėtimo iki lauko uždavinį (žr. § 58).

Vystantis matematikos mokslui (mokslui apie skaičius), skaičių aibių praplėtimo uždaviniai kildavo nuolat. Praplėtus sveikųjų skaičių žiedą $\mathbf{Z}$ iki racionaliųjų skaičių lauko $\mathbf{Q}$, buvo mėginama spręsti lygtį $x^2-2=0$. Paaiškėjo, kad nėra racionaliojo skaičiaus, kuris būtų tos lygties sprendinys. Panašiai, sprendžiant lygtį $x^2+1=0$, buvo konstatuota, kad visoje realiųjų skaičių aibėje $\mathbf{R}$ nėra jos sprendinių. Praplėtus realiųjų skaičių lauką, buvo gautas kompleksinių skaičių laukas (1 d., § 40).

Laukų plėtinių teorija plati ir sudėtinga. Šiame skyriuje pateiksime tik jos pradmenis.

Trumpai priminsime kai kurias sąvokas.

Lauko $\mathbf{L}=(L, +, \cdot)$ *plėtiniu vadinamas kiekvienas laukas* $\mathbf{L}'=(L', +, \cdot)$, $L \subset L'$, *kurio binarės operacijos* $+, \cdot$ *poaibyje* L *sutampa su lauko* $\mathbf{L}$ *operacijomis* $+, \cdot$.

Toliau nagrinėsime tik tokius lauko $\mathbf{L}$ plėtinius, kuriems priklauso laukui $\mathbf{L}$ nepriklausantys elementai $\alpha_1, \ldots, \alpha_n$ ($n \in \mathbf{N}$). Tokių plėtinių jau turėjome. Kompleksinių skaičių laukas yra realiųjų skaičių lauko plėtinys, kuriam priklauso elementas i, $i \notin \mathbf{R}$ ($i^2+1=0$). Polinomas $f(x)=x^2-2$ neišskaidomas lauke $\mathbf{Q}$, jo skaidinio laukas yra minimalus lauko $\mathbf{Q}$ plėtinys, kuriam priklauso $\sqrt{2}$, $\sqrt{2} \notin \mathbf{Q}$.

Lauko $\mathbf{L}$ *plėtinys* $\mathbf{L}^*$, *kuriam priklauso elementai* $\alpha_1, \ldots, \alpha_n$, *vadinamas minimaliuoju plėtiniu, jeigu jis yra lauko* $\mathbf{L}$ *kiekvieno kito plėtinio* $\mathbf{L}'$, *turinčio tuos elementus, polaukis.*

Jeigu $\alpha_1, \ldots, \alpha_n \in \mathbf{L}$ ir yra bent vienas lauko **L** plėtinys **L'**, kuriam priklauso elementai $\alpha_1, \ldots, \alpha_n$, tai yra ir minimalusis plėtinys, turintis elementus $\alpha_1, \ldots, \alpha_n$. Tokį plėtinį gausime paėmę lauko **L** visų plėtinių **L'**, turinčių elementus $\alpha_1, \ldots, \alpha_n$, sankirtą, nes laukų sankirta yra laukas, kiekvieno daugiklio polaukis.

Lauko **L** *minimalusis plėtinys* **L***, *turintis elementus* $\alpha_1, \ldots, \alpha_n$, *vadinamas lauko* **L** *plėtiniu, gautu prijungus elementus* $\alpha_1, \ldots, \alpha_n$. *Jis vadinamas transcendentiniu, jei bent vienas iš elementų* $\alpha_1, \ldots, \alpha_n$ *yra transcendentinis lauko* **L** *atžvilgiu, ir algebriniu, jei visi tie elementai yra algebriniai lauko* **L** *atžvilgiu.*

Aiškinsimės, kaip galima sukonstruoti lauko **L** plėtinį prijungiant elementus $\alpha_1, \ldots, \alpha_n$, kurie nėra lauko **L** elementai. 8 skyriaus 79 paragrafe nustatėme, kad tuo atveju, kai elementai $\alpha_1, \ldots, \alpha_n$ yra transcendentiniai lauko **L** atžvilgiu, n kintamųjų polinominių trupmenų aibė $\mathbf{L}(\alpha_1, \ldots, \alpha_n)$, atitinkamai apibrėžus operacijas su tomis trupmenomis, yra lauko **L** plėtinys, kuriam priklauso ir elementai $\alpha_1, \ldots, \alpha_n$. (Atkreipiame dėmesį, jog čia vietoje $x_1, \ldots, x_n$ rašome $\alpha_1, \ldots, \alpha_n$ norėdami pabrėžti, kad kalbame ne apie bet kokius transcendentinius **L** atžvilgiu elementus, o apie konkretų jų rinkinį.)

Nagrinėsime atvejį, kai elementai $\alpha_1, \ldots, \alpha_n$ yra algebriniai lauko **L** atžvilgiu. $L(\alpha_1, \ldots, \alpha_n)$ žymėsime aibę santykių

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)};$$

čia f, $g \neq O$ – bet kokie polinomai virš **L** ir, be to, $g(\alpha_1, \ldots, \alpha_n) \neq O$ (šiuo atveju $f(\alpha_1, \ldots, \alpha_n)$ ir $g(\alpha_1, \ldots, \alpha_n)$ yra polinomų f ir g reikšmės taške $(\alpha_1, \ldots, \alpha_n)$. Tų santykių operacijas apibrėžę kaip polinominių trupmenų operacijas, nustatome, kad $(L(\alpha_1, \ldots, \alpha_n), +, \cdot)$ yra laukas, kurio polaukis yra **L** ir kuriam priklauso elementai $\alpha_1, \ldots, \alpha_n$, t. y. ir šiuo atveju $\mathbf{L}(\alpha_1, \ldots, \alpha_n)$ yra lauko **L** plėtinys, turintis elementus $\alpha_1, \ldots, \alpha_n$.

Nagrinėjamuoju atveju $\mathbf{L}(\alpha_1, \ldots, \alpha_n)$ yra ne polinominių trupmenų, o polinominių trupmenų reikšmių taške $(\alpha_1, \ldots, \alpha_n)$ laukas.

Išsiaiškinsime, kaip susiję laukas $\mathbf{L}(\alpha_1, \ldots, \alpha_n)$ ir lauko **L** plėtinys, gautas prijungus elementus $\alpha_1, \ldots, \alpha_n$.

178 teorema. *Laukas* $\mathbf{L}(\alpha_1, \ldots, \alpha_n)$ *yra minimalusis lauko* **L** *plėtinys, turintis elementus* $\alpha_1, \ldots, \alpha_n$.

Įrodymas. Tarkime, kad **L'** yra kuris nors lauko **L** plėtinys, turintis elementus $\alpha_1, \ldots, \alpha_n$. Kadangi laukui **L'** priklauso lauko **L** elementai, tai $f(\alpha_1, \ldots, \alpha_n) \in L'$, f – bet kuris polinomas virš **L**, ir

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \in \ ',$$

f, $g \neq O$ ($g(\alpha_1, \ldots, \alpha_n) \neq O$, kai $\alpha_1, \ldots, \alpha_n$ – algebriniai elementai) – bet kurie polinomai virš **L**. Taigi $L(\alpha_1, \ldots, \alpha_n) \subset L'$ ir

$$L(\alpha_1, \ldots, \alpha_n) \subset \cap L'.$$

Kadangi laukui **L** $(\alpha_1, \ldots, \alpha_n)$ priklauso elementai $\alpha_1, \ldots, \alpha_n$ ir jis yra lauko **L** plėtinys, tai

$$\cap L' \subset L(\alpha_1, \ldots, \alpha_n).$$

Pastarieji sąryšiai ir įrodo, kad $L(\alpha_1, \ldots, \alpha_n) = \cap L'$

Taigi iš teoremos išplaukia, kad *polinominių trupmenų laukas* **L** $(\alpha_1, \ldots, \alpha_n)$ *yra transcendentinis lauko* **L** *plėtinys, gautas prijungus (transcendentinius) elementus* $\alpha_1, \ldots, \alpha_n$.

§94. Lauko paprastieji plėtiniai

Lauko **L** *plėtinys* **L** (α) *vadinamas paprastuoju algebriniu plėtiniu, kai elementas* α *yra algebrinis lauko* **L** *atžvilgiu, ir paprastuoju transcendentiniu plėtiniu, kai elementas* α *yra transcendentinis lauko* **L** *atžvilgiu.*

Paprastasis transcendentinis plėtinys **L** (α) yra vieno kintamojo polinominių trupmenų laukas virš **L** – vieno kintamojo polinomų žiedo santykių laukas.

Iš 131 ir 128 teoremų išplaukia šitoks teiginys.

Lauko **L** *kiekvieni du paprastieji transcendentiniai plėtiniai yra izomorfiški.*

Aptarkime detaliau lauko **L** paprastojo algebrinio plėtinio **L** (α) konstrukciją. Nors 178 teorema teigia, kad ir šiuo atveju

$$L(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x),\ g(x) \in L[x],\ g(\alpha) \neq 0 \right\},$$

tačiau pamatysime, jog faktiškai ta aibė gali būti gauta be dalybos. Tarkime, kad α yra algebrinis n-ojo laipsnio, $n > 1$, elementas virš **L**. Jo *minimalusis polinomas* $p_\alpha(x)$ *– pirminis virš* **L** *polinomas, kurio vyriausiasis koeficientas lygus vienetui ir kurio šaknis yra elementas* α – yra n-ojo laipsnio.

179 teorema. *Kiekvienas paprastojo algebrinio plėtinio elementas*

$$\frac{f(\alpha)}{g(\alpha)} \in L(\alpha),\ g(\alpha) \neq 0,$$

išreiškiamas pavidalu

$$\frac{f(\alpha)}{g(\alpha)} = \sum_{j=0}^{n-1} a_j \alpha^j$$

su $a_j \in L$, $j = 0, 1, \ldots, n-1$, *vieninteliu būdu. Čia n yra elemento* α *laipsnis.*

Įrodymas. Jeigu $p_\alpha(x)$ – elemento α minimalusis polinomas, deg $(p_\alpha)=n$, tai $g(x)$ ir $p_\alpha(x)$ – tarpusavyje pirminiai polinomai. Tada pagal 114 teoremą yra tokie polinomai $u(x)$, $v(x)\in L[x]$, su kuriais teisinga lygybė

$$g(x)u(x)+p_\alpha(x)v(x)=e.$$

Iš jos, remdamiesi sąlyga $p_\alpha(\alpha)=O$, gauname

$$g(\alpha)u(\alpha)=e.$$

Todėl

$$\frac{f(\alpha)}{g(\alpha)}=\frac{f(\alpha)u(\alpha)}{g(\alpha)u(\alpha)}=f(\alpha)u(\alpha).$$

Tarkime, kad $\varphi(x)=f(x)u(x)$. Pagal dalybos su liekana teoremą

$$\varphi(x)=p_\alpha(x)q(x)+r(x).$$

Todėl

$$\frac{f(\alpha)}{g(\alpha)}=\varphi(\alpha)=r(\alpha).$$

Polinomas $r(x)$ nustatomas vienareikšmiškai ir deg $(r(x))<n$, arba $r(x)=O(x)$. Todėl išraiška

$$r(x)=\sum_{j=0}^{n-1}a_jx^j,\quad a_j\in L,$$

yra vienintelė. Taigi ir išraiška

$$\frac{f(\alpha)}{g(\alpha)}=\sum_{j=0}^{n-1}a_j\alpha^j,\quad a_j\in L,$$

vienintelė.

1 išvada. *Kai α yra n-ojo laipsnio algebrinis* **L** *atžvilgiu elementas, lauko* **L** *paprastojo algebrinio plėtinio* **L** (α) *bazinė aibė yra*

$$\left\{\sum_{j=0}^{n-1}a_j\alpha^j \mid a_j\in L,\quad j=0,\ 1,\ \ldots,\ n-1\right\}.$$

Lauko **L** *paprastasis algebrinis plėtinys* **L** (α), *gautas prijungus n-ojo laipsnio algebrinį* **L** *atžvilgiu elementą α, vadinamas paprastuoju algebriniu n-ojo laipsnio plėtiniu.*

179 teoremos 1 išvada visiškai aprašo tokio plėtinio bazinės aibės konstrukciją. Toji aibė yra visų ne aukštesnio kaip $n-1$-ojo laipsnio polinomų virš **L** reikšmių taške α aibė.

Pavyzdžiai. 1. Kadangi i yra polinomo x^2+1 šaknis, tai i yra 2-ojo laipsnio algebrinis elementas realiųjų skaičių lauko **R** atžvilgiu. Todėl $n=2$, ir

$$\mathbf{R}(i)=(\{a+ib \mid a,\ b\in\mathbf{R}\},\ +,\ \cdot)=\mathbf{K}$$

– kompleksinių skaičių laukas yra realiųjų skaičių lauko paprastasis algebrinis antrojo laipsnio plėtinys.

2. Aritmetinė reikšmė $\sqrt[4]{2}$ yra polinomo x^4-2 šaknis. Todėl $\mathbf{Q}(\sqrt[4]{2})=\{a+b\sqrt[4]{2}+c\sqrt[4]{4}+d\sqrt[4]{8} \mid a,\ b,\ c,\ d\in\mathbf{Q}\}$.

2 išvada. *Jeigu* **L** *yra pirminis charakteristikos p laukas, o* α *yra algebrinis n-ojo laipsnio* **L** *atžvilgiu elementas, tai lauko* **L** (α) *bazinė aibė turi* p^n *elementų.*

Įrodymas. Kadangi išraiškoje

$$\sum_{j=0}^{n-1} a_j\alpha^j,\ a_j\in L,\ \ j=0,\ 1,\ \ldots,\ n-1,$$

kiekvienas koeficientas a_j gali įgyti p skirtingų reikšmių, tai suma gali įgyti p^n skirtingų reikšmių.

Atkreipiame dėmesį į tai, kad sudedant ir atimant aibės

$$\left\{\sum_{j=0}^{n-1} a_j\alpha^j \mid a_j\in L.\ \ j=0,\ 1,\ \ldots,\ n-1\right\}$$

elementus jokių komplikacijų nekyla. Dauginant gali tekti remtis šitokiais samprotavimais. Jeigu

$$\sum_{j=0}^{n-1} a_j\alpha^j.\ \sum_{k=0}^{n-1} b_k\alpha^k=\varphi(\alpha)$$

ir $\deg\varphi(x)\geqslant n$, tai užrašę $\varphi(x)=p\alpha(x)\,q(x)+r(x)$, $p_\alpha(x)$ – elemento α minimalusis polinomas, gausime $\varphi(\alpha)=r(\alpha)=\sum_{j=0}^{n-1} c_j\alpha^j$, nes $r(x)$ laipsnis mažesnis už n arba $r(x)=o(x)$. Tos aibės elementų dalyba yra ne kas kita, o iracionalumo trupmenos vardiklyje naikinimas.

180 teorema. *Jeigu* α *ir* β *yra algebriniai lauko* **L** *atžvilgiu elementai ir turi tą patį minimalųjį polinomą* $p(x)$, *tai paprastieji algebriniai plėtiniai* **L** (α) *ir* **L** (β) *yra izomorfiški ir egzistuoja toks jų izomorfizmas* φ, *kad* $\varphi(a)=a$ *su visais* $a\in L$ *ir* $\varphi(\alpha)=\beta$.

Įrodymas. Jeigu n yra polinomo $p(x)$ laipsnis, tai pagal 179 teoremą kiekvienas plėtinio **L** (α) elementas yra

$$\sum_{j=0}^{n-1} a_j\alpha^j$$

pavidalo, o kiekvienas plėtinio $\mathbf{L}(\beta)$ elementas –

$$\sum_{j=0}^{n-1} b_j \beta^j$$

pavidalo.

Bijekcija

$$\varphi\left(\sum_{j=0}^{n-1} a_j \alpha^j\right) = \sum_{j=0}^{n-1} a_j \beta^j$$

yra tokia, kad $\varphi(a) = a$ su kiekvienu $a \in L$ ir

$$\varphi(\alpha) = \beta.$$

Kadangi sudėtis ir daugyba laukuose $\mathbf{L}(\alpha)$ ir $\mathbf{L}(\beta)$ yra apibrėžta, kaip ir polinomų žiede $\mathbf{L}[x]$, tai ta bijekcija yra izomorfizmas.

181 teorema. *Jeigu α minimalusis polinomas yra $p(x)$, tai paprastasis algebrinis plėtinys $\mathbf{L}(\alpha)$ yra izomorfiškas polinomų žiedo $\mathbf{L}[x]$ faktoržiedui $\mathbf{L}[x]/(p)$ pagal idealą $(p(x))$.*

Įrodymas. Lauko $\mathbf{L}(\alpha)$ elementui

$$a = \sum_{j=0}^{n-1} a_j \alpha^j$$

(čia $n = \deg p$) priskirsime liekanų klasę $[r]_p$ moduliu $p(x)$, t. y.

$$\varphi\left(\sum_{j=0}^{n-1} a_j \alpha^j\right) = [r]_p;$$

čia

$$r(x) = \sum_{j=0}^{n-1} a_j x^j.$$

Ta funkcija yra bijekcija. Kadangi

$$a + b = \sum_{j=0}^{n-1} a_j \alpha^j + \sum_{j=0}^{n-1} b_j \alpha^j = \sum_{j=0}^{n-1} (a_j + b_j) \alpha^j,$$

tai $\varphi(a+b) = \varphi(a) + \varphi(b)$. Be to,

$$ab = \left(\sum_{j=0}^{n-1} a_j \alpha^j\right)\left(\sum_{i=0}^{n-1} b_i \alpha^i\right) = \sum_{j=0}^{n-1} c_j \alpha^j;$$

čia $c_0, c_1, \ldots, c_{n-1}$ yra liekanos $r(x)$ koeficientai išraiškoje

$$\left(\sum_{j=0}^{n-1} a_j x^j\right)\left(\sum_{i=0}^{n-1} b_i x^i\right)=p(x)\,q(x)+r(x),$$

todėl $\varphi(ab)=\varphi(a)\,\varphi(b)$.

Taigi apibrėžtoji bijekcija yra izomorfizmas.

Prisiminę laukų izomorfizmo teoremą (žr. 1 d., 24 teoremą) ir tai, kad algebrinio elemento minimalusis polinomas yra pirminis, gauname išvadą.

Polinomų žiedo $\mathbf{L}[x]$ *faktoržiedas* $\mathbf{L}[x]/(p)$ *pagal pirminį polinomą* $p(x)$ *yra laukas* (*palyginkite su* 111 *teorema*).

Uždaviniai

1. Įrodykite: jeigu elementai α ir β yra transcendentiniai $\mathbf{L}$ atžvilgiu, tai $\mathbf{L}(\alpha)\cong\mathbf{L}(\beta)$ ir egzistuoja toks izomorfizmas φ, kad $\varphi(a)=a$ su kiekvienu $a\in L$ ir $\varphi(\alpha)=\beta$.

2. Užrašykite plėtinių bazines aibes:

1) $\mathbf{Q}(i)$; 2) $\mathbf{Q}(\sqrt[3]{5})$; 3) $\mathbf{Q}(\sqrt[3]{2}+\sqrt{3})$;

4) $\mathbf{Q}\left(\frac{\sqrt[3]{2}}{\sqrt{3}}\right)$; 5) $\mathbf{Q}\left(\frac{\sqrt[3]{3}+\sqrt{2}}{\sqrt[3]{5}}\right)$.

3. Raskite laukui $\mathbf{Q}(\sqrt[3]{2})$ izomorfiškus laukus.

§95. Lauko kartotiniai algebriniai plėtiniai

Lauko $\mathbf{L}$ minimalusis plėtinys $\mathbf{L}(\alpha_1, \ldots, \alpha_n)$, kai $\alpha_1, \ldots, \alpha_n$ yra algebriniai $\mathbf{L}$ atžvilgiu, $n\geqslant 2$, vadinamas lauko $\mathbf{L}$ *kartotiniu algebriniu plėtiniu.*

Šiame paragrafe įsitikinsime, kad lauko $\mathbf{L}$ kiekvienas kartotinis algebrinis plėtinys yra jo paprastasis algebrinis plėtinys. Pirmiausia įrodysime šitokią lemą.

Lema. *Jeigu elementai* α *ir* β *yra algebriniai lauko* $\mathbf{L}$ *atžvilgiu, tai su kiekvienu* $c\in L$ *elementas* $\alpha+c\beta$ *irgi algebrinis lauko* $\mathbf{L}$ *atžvilgiu.*

Įrodymas. Kai $c=O$, tvirtinimas akivaizdus. Kai $c\neq O$, $c\beta$ yra algebrinis $\mathbf{L}$ atžvilgiu, nes jeigu

$$\sum_{j=0}^{m} b_j\beta^j=O,$$

tai ir

$$\sum_{j=0}^{m} (b_j c^{-j})(c\beta)^j = O.$$

Taigi užtenka įrodyti, kad algebrinių elementų α ir $c\beta$ suma yra algebrinis elementas lauko **L** atžvilgiu.

Elemento α minimalųjį polinomą žymėsime $p_1(x)$, to polinomo šaknis – $\alpha_1=\alpha, \alpha_2, \ldots, \alpha_n$, o elemento $c\beta$ minimalųjį polinomą – $p_2(x)$, jo šaknis – $\beta_1=c\beta, \beta_2, \ldots, \beta_m$.

Reiškinys

$$f(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-(\alpha_i+\beta_j))$$

yra simetrinis pagal dvi sistemas $\alpha_1, \ldots, \alpha_n$ ir $\beta_1, \ldots, \beta_m$ polinomas. Todėl pagal 167 teoremos išvadą polinomo $f(x)$ koeficientai yra lauko **L** elementai. Kadangi jo šaknys yra $\alpha_i+\beta_j$ $(i=1, \ldots, n, j=1, \ldots, m)$, tai $\alpha_1+\beta_1=\alpha+c\beta$ yra šaknis. Taigi $\alpha+c\beta$ yra algebrinis **L** atžvilgiu elementas.

182 teorema. *Jeigu* **L** *yra nulinės charakteristikos laukas, tai kiekvienas algebrinis kartotinis plėtinys* $\mathbf{L}(\alpha_1, \ldots, \alpha_n)$ *yra paprastas, t. y. egzistuoja toks algebrinis* **L** *atžvilgiu elementas* α, *kad*

$$\mathbf{L}(\alpha_1, \ldots, \alpha_n)=\mathbf{L}(\alpha).$$

Įrodymas. Pirmiausia įrodysime teoremą, kai $n=2$.

Tarkime, kad α_1 yra pirminio polinomo $p_1(x)$ šaknis ir β_1 yra pirminio polinomo $p_2(x)$ šaknis. Skirtingas polinomo $p_1(x)$ šaknis žymėsime $\alpha_1, \ldots, \alpha_n$, o skirtingas polinomo $p_2(x)$ šaknis – $\beta_1, \ldots, \beta_m$.

Kai $k\neq 1$, $\beta_k\neq\beta_1$, lygtis

$$\alpha_i + c\,\beta_k \neq \alpha_1 + c\,\beta_1$$

su kiekvienu i ir kiekvienu $k\neq 1$ lauke **L** turi ne daugiau kaip po vieną sprendinį. Paėmę $c\in L$ skirtingą nuo tų lygčių sprendinių (tai galime padaryti, nes lauko **L** charakteristika lygi nuliui), su kiekvienu $k\neq 1$ ir kiekvienu i turėsime

$$\alpha_i + c\,\beta_k \neq \alpha_1 + c\,\beta_1.$$

Elementas

$$\alpha=\alpha_1+c\,\beta_1$$

priklauso laukui $\mathbf{L}(\alpha_1, \beta_1)$, taigi pagal lemą α yra algebrinis **L** atžvilgiu.

Kadangi $p_2(\beta_1)=O$ ir $p_1(\alpha-c\beta_1)=p_1(\alpha)=O$, tai polinomai $p_2(x)$ ir $p_1(\alpha-cx)$ turi bendrą šaknį β_1. Daugiau bendrų šaknų tie polinomai neturi, nes pagal c parinkimą

$$\alpha - c\,\beta_k \neq \alpha_i, \quad i=2, \ldots, n,$$

todėl

$$p_1(\alpha - c\,\beta_k)\neq 0, \quad k\neq 1.$$

Taigi $D(p_2(x), p_1(\alpha-cx))=(x-\beta_1)^s$; čia s yra polinomų $p_2(x)$ ir $p_1(\alpha-cx)$ bendros šaknies β_1 kartotinumas. Kadangi $p_2(x)$ ir $p_1(\alpha-cx)$ yra polinomai virš **L** (α) (žr. § 72), $(x-\beta_1)^s$ taip pat yra polinomas virš **L** (α). Iš to išplaukia, kad $\beta_1 \in L(\alpha)$.

Bet $\alpha_1=\alpha-c\beta_1$, taigi ir $\alpha_1 \in L(\alpha)$. Todėl

$$L(\alpha_1, \beta_1) \subset L(\alpha).$$

Kadangi $\alpha=\alpha_1+c\beta_1$, tai $\alpha \in L(\alpha_1, \beta_1)$, todėl ir

$$L(\alpha) \subset L(\alpha_1, \beta_1).$$

Nustatėme, kad egzistuoja toks algebrinis L atžvilgiu elementas α, kad

$$L(\alpha_1, \beta_1)=L(\alpha).$$

Kai $n>2$, remdamiesi išraiška

$$L(\alpha_1, \ldots, \alpha_n)=L(\alpha_1, \alpha_2)(\alpha_3, \ldots, \alpha_n)$$

ir pirmąja įrodymo dalimi, gausime tokį algebrinį L atžvilgiu elementą β_1, kad

$$L(\alpha_1, \ldots, \alpha_n)=L(\beta_1)(\alpha_3, \ldots, \alpha_n)=L(\beta_1, \alpha_3, \ldots, \alpha_n).$$

Taip samprotaudami, po $n-1$ žingsnio rasime tokį elementą α, algebrinį **L** atžvilgiu, kad bus $L(\alpha_1, \ldots, \alpha_n)=L(\alpha)$.

§96. Baigtiniai ir algebriniai plėtiniai

Laukų plėtinių yra įvairių. Trumpai išnagrinėjome paprastuosius ir kartotinius algebrinius plėtinius. Susipažinsime su lauko baigtiniais plėtiniais.

Lauko **L** *plėtinys* **P** *vadinamas baigtiniu, jei yra tokie lauko* **P** *elementai* $\alpha_1, \ldots, \alpha_n$, *kad bet kurį lauko* **P** *elementą* β *galima užrašyti šitaip*:

$$\beta=a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n;$$

čia $a_1, a_2, \ldots, a_n$ – *lauko* **L** *elementai.*

Baigtinis lauko **L** *plėtinys yra vektorinė erdvė virš* **L**. (Šį teiginį paliekame įrodyti skaitytojui.)

Tos vektorinės erdvės dimensija vadinama baigtinio plėtinio **P** *laipsniu* ir žymima (**P** : **L**). Laikysime, kad apibrėžime minimų elementų $\alpha_1, \ldots, \alpha_n$ skaičius n lygus plėtinio **P** laipsniui: $n=(\mathbf{P} : \mathbf{L})$. Taip ir bus, jei imsime tiesiškai nepriklausomus elementus $\alpha_1, \ldots, \alpha_n$.

Pavyzdžiai. 1. Kompleksinių skaičių laukas **K** yra baigtinis antrojo laipsnio realiųjų skaičių lauko **R** plėtinys, nes $(\forall \alpha \in \mathbf{K})$ $(\exists a, b \in \mathbf{R})$ $\alpha=a+ib$, o 1 ir i yra tiesiškai nepriklausomi. Tai išplaukia iš teiginio: jeigu $x+iy=0$, tai $x=y=0$.

2. $\mathbf{Q}(\sqrt[3]{2})$ yra baigtinis trečiojo laipsnio racionaliųjų skaičių lauko plėtinys. Kadangi

$$\mathbf{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,\ b,\ c\in\mathbf{Q}\},$$

o $1,\ \sqrt[3]{2},\ \sqrt[3]{4}\in\mathbf{Q}(\sqrt[3]{2})$ ir $x=y=z=0$, kai $x+y\sqrt[3]{2}+z\sqrt[3]{4}=0$, tai $1,\ \sqrt[3]{2},\ \sqrt[3]{4}$ – tiesiškai nepriklausomi ir $n=3$.

183 teorema. *Lauko* **L** *kiekvienas paprastasis algebrinis n-ojo laipsnio plėtinys yra baigtinis n-ojo laipsnio plėtinys.*

Įrodymas. Pagal 179 teoremą

$$(\forall\,\beta\in\mathbf{L}(\alpha))(\exists\,a_0,\ a_1,\ \ldots,\ a_{n-1}\in\mathbf{L})\ \beta=\sum_{j=0}^{n-1}a_j\alpha^j.$$

Tai reiškia, kad $\mathbf{L}(\alpha)_j$ – baigtinis lauko **L** plėtinys. Kadangi

$$\sum_{j=0}^{n-1}x_j\alpha^j=0$$

tik tada, kai $x_j=0$, $j=0,\ 1,\ \ldots,\ n-1$, tai elementai $e,\ \alpha^1,\ \alpha^2,\ \ldots,\ \alpha^{n-1}$ yra tiesiškai nepriklausomi. Taigi $(\mathbf{L}(\alpha):\mathbf{L})=n$.

Lauko **L** *plėtinys* **P** *vadinamas algebriniu, jei kiekvienas lauko* **P** *elementas yra algebrinis* **L** *atžvilgiu.*

Pavyzdys. Kompleksinių skaičių laukas **K** yra realiųjų skaičių lauko algebrinis plėtinys, nes $a+ib$ yra lygties $x^2-2ax+(a^2+b^2)=0$ sprendinys.

184 teorema. *Lauko* **L** *kiekvienas baigtinis plėtinys yra algebrinis to lauko plėtinys.*

Įrodymas. Tarkime, kad **P** – lauko **L** baigtinis n-ojo laipsnio plėtinys ir $\beta\in\mathbf{P}$. Kadangi **P** – n-matė vektorinė erdvė virš **L**, tai kiekvieni $n+1$ aibės **P** elementai yra tiesiškai priklausomi. Todėl tiesiškai priklausomi yra ir elementai $e=\beta^0,\beta,\ \ldots,\beta^n$. Taigi yra toks nenulinis lauko **L** elementų rinkinys $a_0,\ a_1,\ \ldots,\ a_n$, su kuriuo

$$\sum_{j=0}^{n}a_j\beta^j=0.$$

Pastaroji lygybė reiškia, kad β yra polinomo

$$\sum_{j=0}^{n} a_j x^j \in L[x]$$

šaknis – algebrinis **L** atžvilgiu elementas.

§97. Algebrinių skaičių aibės savybės

Klasikinės algebros pagrindinė teorema teigia, kad kompleksinių skaičių laukas yra algebriškai uždaras. Iš to išplaukia, kad visi racionaliųjų skaičių lauko **Q** atžvilgiu algebriniai elementai yra skaičiai (realieji arba menamieji). Kiekvieną polinomą su racionaliaisiais koeficientais $\varphi(x) \in \mathbf{Q}[x]$ galima išreikšti $\varphi(x) = cf(x)$ pavidalu; čia $c \in \mathbf{Q}$, $f(x)$ – polinomas su sveikaisiais koeficientais. Asocijuotųjų polinomų šaknys sutampa. Todėl galime pateikti šitokius apibrėžimus.

Skaičius α vadinamas algebriniu, jei jis yra kokio nors nenulinio laipsnio polinomo su sveikaisiais koeficientais šaknis.

Skaičius α vadinamas transcendentiniu, jei jis nėra jokio nenulinio laipsnio polinomo su sveikaisiais koeficientais šaknis.

Pavyzdžiai. 1. Skaičiai $\sqrt{2}$, $\sqrt[3]{5}$, $\frac{2-\sqrt{3}}{2}$ yra algebriniai, nes jie yra polinomų x^2-2, x^3-5, $4x^2-8x+1$ šaknys.

2. Skaičius $3-2i$ – algebrinis, nes yra polinomo $x^2-6x+13$ šaknis.

Transcendentinių skaičių pavyzdžių pateiksime vėliau, išsprendę jų egzistavimo uždavinį.

185 teorema. *Algebrinių skaičių aibė sudaro lauką.*

Įrodymas. Pažymėkime K_a kompleksinių algebrinių skaičių aibę. Aišku, kad $K_a \subset K$. Kadangi **K** – laukas, tai užtenka įsitikinti, kad teisingas šitoks teiginys:

$$(\forall \alpha,\ \beta \in K_a)\ \alpha+\beta \in K_a,\ \alpha-\beta \in K_a,\ \alpha\beta \in K_a,\ \frac{\alpha}{\beta} \in K_a,\ \text{kai}\ \beta \neq 0.$$

Iš 95 paragrafo lemos išplaukia, kad algebrinių skaičių α ir β suma $\alpha+\beta$ ir skirtumas $\alpha-\beta$ yra algebriniai skaičiai. Todėl lieka įrodyti, kad $\alpha\beta$ ir $\frac{\alpha}{\beta}$ ($\beta \neq 0$) yra algebriniai skaičiai, kai α ir β – algebriniai skaičiai.

Tarkime, kad $\alpha=\alpha_1$ yra n-ojo laipsnio algebrinis skaičius ir jo minimalusis polinomas yra $p_1(x)$, o $\beta=\beta_1$ yra m-ojo laipsnio algebrinis skaičius ir jo minimalusis polinomas – $p_2(x)$. Polinomo $p_1(x)$ šaknis žymėsime $\alpha_1, \ldots, \alpha_n$ ir polinomo $p_2(x)$ šaknis – $\beta_1, \ldots, \beta_m$.

Kadangi išraiška

$$g(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j)$$

nekinta bet kaip sukeitus vietomis $\alpha_1, \ldots, \alpha_n$ ir bet kaip sukeitus $\beta_1, \ldots, \beta_m$, tai pagal 167 teoremą polinomo $g(x)$ koeficientai yra racionalieji skaičiai. Todėl visi $\alpha_i\beta_j$ $(i=1, \ldots, n, j=1, \ldots, m)$ yra algebriniai skaičiai, kurių laipsnis ne didesnis už nm. Vadinasi, $\alpha_1\beta_1$ taip pat yra algebrinis skaičius.

Kadangi $\frac{\alpha}{\beta}=\alpha\left(\frac{1}{\beta}\right)$, kai $\beta\neq 0$, tai užtenka įrodyti, kad $\frac{1}{\beta}$ yra algebrinis skaičius, ir toliau reikia remtis pirmąja įrodymo dalimi.

Tarkime, kad β yra polinomo su racionaliaisiais koeficientais

$$\sum_{j=0}^{m}a_jx^j$$

šaknis, t. y.

$$\sum_{j=0}^{m}a_j\beta^j=0.$$

Kai $\beta\neq 0$,

$$\sum_{j=0}^{m}a_j\beta^j=\beta^m\sum_{j=0}^{m}a_j\left(\frac{1}{\beta}\right)^{m-j}=0,$$

t. y. $\frac{1}{\beta}$ yra polinomo

$$\sum_{j=0}^{m}a_jx^{m-j}$$

šaknis. Taigi $\frac{1}{\beta}$, o kartu ir $\frac{\alpha}{\beta}$ yra algebriniai skaičiai.

Išvada. *Realieji algebriniai skaičiai sudaro lauką – realiųjų skaičių lauko polaukį.*

Tą išvadą gauname iš teoremos: kai α ir β realieji skaičiai, $\alpha\pm\beta$, $\alpha\beta$ ir $\frac{\alpha}{\beta}$, kai $\beta\neq 0$, taip pat realieji skaičiai.

186 teorema. *Algebrinių skaičių laukas yra algebriškai uždaras.*

Įrodymas. Užtenka įrodyti, kad bet kokio polinomo $f(x)$ $(\deg(f)\geqslant 1)$ virš algebrinių skaičių lauko kiekviena šaknis yra algebrinis skaičius.

Tarkime, kad

$$f(x)=\sum_{k=0}^{n} a_k x^k$$

yra nenulinio laipsnio polinomas, kurio koeficientai – algebriniai skaičiai. Koeficientui a_k, $k=0, 1, \ldots, n$, jungtinius skaičius, t. y. to paties minimaliojo polinomo šaknis, žymėsime

$$a_k^{(1)}, a_k^{(2)}, \ldots, a_k^{(m_k)}$$

(čia $a_k^{(1)}=a_k$, m_k – algebrinio skaičiaus a_k laipsnis) ir sudarysime visus galimus polinomus

$$f_{j_0\ldots j_n}(x)=\sum_{k=0}^{n} a_k^{(j_k)} x^k, \quad f(x)=f_{1\ldots 1}(x);$$

čia indeksai j_k, nepriklausomai vienas nuo kito, įgyja visas reikšmes $1, 2, \ldots, m_k$. Tų polinomų sandaugos

$$F(x)=\prod f_{j_0\ldots j_n}(x)$$

koeficientas

$$A_l, \quad l=0, 1, \ldots, n\sum_{k=0}^{n} m_k,$$

yra simetrinis polinomas pagal koeficientų

$$a_k^{(1)}, \ldots, a_k^{(m_k)}, \quad k=0, 1, \ldots, n,$$

sistemas. $n+1$ kartą remdamiesi 164 ir 167 teoremomis nustatome, kad polinomo $F(x)$ koeficientai yra racionalieji skaičiai. Todėl polinomo $F(x)$ šaknys – algebriniai skaičiai. Kadangi polinomas $f(x)$ yra vienas iš polinomo $F(x)$ daliklių, tai jo šaknys irgi algebriniai skaičiai.

Algebrinis skaičius, kurio minimalusis polinomas yra polinomas su sveikaisiais koeficientais, vadinamas sveikuoju algebriniu skaičiumi.

187 teorema. *Sveikieji algebriniai skaičiai sudaro žiedą.*

Įrodymas. Užtenka pastebėti, kad 95 paragrafo lemos ir 185 teoremos įrodyme vartoti polinomai $f(x)$ ir $g(x)$ šiuo atveju yra polinomai su sveikaisiais koeficientais ir vyriausiuoju koeficientu, lygiu vienetui.

Polinomo

$$\sum_{k=0}^{m} a_k x^{m-k}$$

vyriausiasis koeficientas a_0 nebūtinai lygus vienetui, kai polinomo

$$\sum_{k=0}^{m} a_k x^k$$

vyriausiasis koeficientas yra vienetas. Iš to išplaukia, kad sveikieji algebriniai skaičiai nesudaro lauko. Taigi ne kiekvienas sveikasis algebrinis skaičius turi atvirkštinį sveikąjį algebrinį skaičių.

Pavyzdžiai. $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[5]{7}$ yra sveikieji algebriniai skaičiai, nes jų minimalieji polinomai yra atitinkamai x^2-2, x^3-2, x^5-7.

$(\sqrt{2})^{-1}=\frac{\sqrt{2}}{2}$ jau nėra sveikasis algebrinis skaičius, nes jo minimalusis polinomas $x^2-\frac{1}{2}$ nėra polinomas su sveikaisiais koeficientais. Skaičių $(\sqrt[3]{2})^{-1}$ ir $(\sqrt[5]{7})^{-1}$ minimalieji polinomai yra $x^3-\frac{1}{2}$, $x^5-\frac{1}{7}$. Todėl tie skaičiai nėra sveikieji algebriniai skaičiai.

§98. Realiųjų transcendentinių skaičių egzistavimas

59 paragrafe apibrėžėme transcendentinius lauko (integralumo srities) atžvilgiu elementus. 60 paragrafe sukonstravome transcendentinį elementą duotosios integralumo srities atžvilgiu. Tuo remdamiesi, galime konstatuoti, kad seka (0, 1, 0, 0, ...) yra elementas, transcendentinis racionaliųjų skaičių lauko **Q** ir sveikųjų skaičių žiedo **Z** atžvilgiu. 97 paragrafe išaiškinome, kokią algebrinę struktūrą sudaro realieji algebriniai skaičiai. Tačiau liko atsakyti į klausimą, ar yra transcendentinių realiųjų ar menamųjų skaičių.

Vienas transcendentinių realiųjų skaičių egzistavimo įrodymas yra jų konstravimas naudojantis grandininėmis tupmenomis. Pirmiausia išsiaiškinkime, kokiu tikslumu realiuosius algebrinius skaičius, kurių laipsnis ne mažesnis už 2, galima aproksimuoti racionaliaisiais skaičiais. Tuo tikslu įrodysime *Liuvilio* (Ž. Liouville, 1809–1882, prancūzų matematikas) teoremą. Po to, remdamiesi ta teorema, galėsime sudaryti tokią grandininę trupmeną, kurios reikšmė nėra algebrinis skaičius.

Nagrinėdami grandinines trupmenas, nustatėme: jeigu skaičiaus α skleidinys grandinine trupmena yra

$$\alpha=[q_0, q_1, \ldots, q_n, \ldots]$$

ir

$$R_n=\frac{P_n}{Q_n}$$

yra to skleidinio n-osios eilės reduktas, tai

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\frac{1}{Q_n^2}.$$

Kokio mažumo, palyginus su vardikliu, gali būti skirtumas

$$\left| \alpha - \frac{a}{b} \right|,$$

kai α yra n-ojo laipsnio algebrinis (realusis) skaičius, kol kas dar neaišku. Toliau pateikiama teorema nustato, už ką negali būti mažesnis tas skirtumas.

Liuvilio teorema. *Kiekvieną realųjį algebrinį skaičių α, kurio laipsnis n ne mažesnis už du, atitinka toks teigiamas skaičius c, su kuriuo teisinga nelygybė*

$$\left| \alpha - \frac{a}{b} \right| \geqslant \frac{c}{b^n},$$

kad ir kokia būtų trupmena $\frac{a}{b}$ $(b \neq 0)$.

Įrodymas. Tarkime, kad α yra polinomo

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

su sveikaisiais koeficientais šaknis. Tada (žr. Bezu teoremą)

$$f(x) = (x - \alpha) g(x), \tag{11.1}$$

$g(x)$ – polinomas su realiaisiais koeficientais, $\deg(g) = n-1$.

Kadangi

$$f\left(\frac{a}{b}\right) = \sum_{k=0}^{n} a_k \left(\frac{a}{b}\right)^k = \frac{1}{b^n} \sum_{k=0}^{n} a_k a^k b^{n-k},$$

skaičiai a, b, a_k, $k=0, \ldots, n$, yra sveikieji, be to, $f\left(\frac{a}{b}\right) \neq 0$, o

$$\sum_{k=0}^{n} a_k a^k b^{n-k}$$

taip pat nelygus nuliui sveikasis skaičius, tai

$$\left| f\left(\frac{a}{b}\right) \right| \geqslant \frac{1}{b^n}.$$

Todėl, (11.1) lygybėje įrašę $x = \frac{a}{b}$ ir pasinaudoję pastarąja nelygybe, gauname

$$\left| \frac{a}{b} - \alpha \right| \geqslant \frac{1}{b^n} \cdot \frac{1}{\left| g\left(\frac{a}{b}\right) \right|}.$$

Jeigu $\frac{a}{b} \subset [\alpha - 1, \alpha + 1]$, tai, pažymėję

$$\frac{1}{c_1} = \max_{l \in [\alpha-1, \alpha+1]} |g(l)|,$$

iš pastarosios nelygybės gauname

$$\left| \frac{a}{b} - \alpha \right| \geqslant \frac{c_1}{b_n}.$$

Kai $\frac{a}{b} \in [\alpha - 1, \alpha + 1]$, tada

$$\left| \frac{a}{b} - \alpha \right| > 1 \geqslant \frac{1}{b^n},$$

nes $b \geqslant 1$. Todėl su bet kokia trupmena $\frac{a}{b}$, pažymėję $c = \min\{1, c_1\}$, gauname nelygybę

$$\left| \frac{a}{b} - \alpha \right| \geqslant \frac{c}{b^n}.$$

188 teorema. *Egzistuoja realieji transcendentiniai skaičiai.*

Įrodymas. Sudarome grandininę trupmeną

$$\alpha = [q_0, q_1, q_2, \ldots, q_n, \ldots],$$

kuri turi savybę

$$q_{k+1} > Q_k^k, \quad k = 0, 1, 2, \ldots$$

Tada teisingos nelygybės

$$\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k Q_{k+1}} = \frac{1}{Q_k (q_{k+1} Q_k + Q_{k-1})} < \frac{1}{q_{k+1} Q_k^2} < \frac{1/Q_k^2}{Q_k^k}.$$

Kadangi $Q_k \to \infty$, kai $k \to \infty$, tai paėmę bet kurį $c > 0$ visada galėsime rasti tokį n, kad būtų

$$\frac{1}{Q_n^2} < c.$$

Todėl, kai $k \geqslant n$,

$$\left| \alpha - \frac{P_k}{Q_k} \right| < \frac{c}{Q_k^n} \quad (k \geqslant n).$$

Nustatėme, kad sukonstruotąjį skaičių α su kiekvienu $c > 0$ atitinka tokia trupmena

$$\frac{a}{b}, \quad \frac{a}{b} = \frac{P_n}{Q_n},$$

su kuria nelygybė

$$\left| \alpha - \frac{a}{b} \right| \leqslant \frac{c}{b^n}$$

teisinga su kiekvienu natūriniu n.

Įrodysime, kad tas skaičius α yra transcendentinis. Tarkime priešingai, α yra algebrinis m-ojo laipsnio skaičius. Tada pagal Liuvilio teoremą kiekviena trupmena $\frac{a}{b}$ tenkintų nelygybę

$$\left|\alpha-\frac{a}{b}\right| \geqslant \frac{c}{b^m},$$

kuri prieštarautų gautajai nelygybei, kai $n \geqslant m$. Gautoji prieštara rodo, kad prielaida klaidinga. Taigi α — transcendentinis skaičius.

Pavyzdys. Imkime skaičių

$$\alpha=\frac{1}{10}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\ldots+\frac{1}{10^{k!}}+\ldots=0{,}1100010\ldots$$

Paėmę bet kokį $n \geqslant 1$ ir $c>0$, galime rasti tokį k, kad būtų $k \geqslant n$ ir $10^{k!} \geqslant \frac{2}{c}$. Kai

$$a=10^{k!}\left(\frac{1}{10}+\frac{1}{10^{2!}}+\ldots+\frac{1}{10^{k!}}\right), \quad b=10^{k!},$$

turime

$$\left|\alpha-\frac{a}{b}\right|=\frac{1}{10^{(k+1)!}}+\frac{1}{10^{(k+2)!}}+\ldots<\frac{1}{10^{(k+1)!}}\left(1+\frac{1}{2}+\frac{1}{2^2}+\ldots\right)=$$

$$=\frac{2}{10^{k!}}\,\frac{1}{10^{k!\,k}} \leqslant \frac{c}{b^n}.$$

Taigi skaičius α yra transcendentinis.

Teoremos įrodymas ne tik patvirtina faktą, kad egzistuoja realieji transcendentiniai skaičiai, bet yra ir metodas kai kuriems iš jų konstruoti.

Skaičiai α, *su kuriais nelygybė*

$$\left|\alpha-\frac{a}{b}\right|<\frac{c}{b^n},$$

kai $n \geqslant 1$ — *bet koks natūrinis skaičius ir* $c>0$, *turi sveikąjį sprendinį* (a, b), *vadinami transcendentiniais Liuvilio skaičiais.*

Liuvilio teorema įrodyta tik 1844 m. Iki to laiko nebuvo žinoma, ar egzistuoja transcendentiniai skaičiai.

Remiantis Liuvilio teorema, neįmanoma nustatyti, algebriniai ar transcendentiniai yra kai kurie praktikoje plačiai vartojami skaičiai, pavyzdžiui π, e ir kt. Todėl nemažai pastangų įdėta siekiant išaiškinti tų ir kitų skaičių transcendentiškumą. 1873 m. prancūzų matematikas *Hermitas* (Š. Hermite, 1822–1901) įrodė, kad skaičius e yra transcendentinis. 1882 m. vokiečių matematikas *Lindemanas* (F. Lindemann, 1852–1939) įrodė plačios klasės skaičių, tarp jų ir π, transcendentiškumą. Žymų indėlį į transcendentinių skaičių teoriją įnešė rusų matematikas *Gelfondas* (A. Gelfond, 1906–1968). Jis įrodė, kad β^{α} pavidalo skaičiai, kai β — nei 0, nei 1 nelygus algebrinis skaičius, o α — iracionalusis algebrinis skaičius, yra transcendentiniai. Pavyzdžiui, skaičiai $2^{\sqrt{2}}$, $(\sqrt{3})^{\sqrt{2}}$ ir pan. yra transcendentiniai.

Šiuo metu žinoma daug transcendentinių skaičių klasių. Vadovėlyje nėra galimybių supažindinti su gana sudėtingais tokių klasių gavimo metodais.

Kitame paragrafe nustatysime, kuri aibė gausesnė – algebrinių realiųjų skaičių ar transcendentinių realiųjų skaičių. Naudosimės vokiečių matematiko *Kantoro* (G. Cantor, 1845–1918) 1874 metais pateiktu realiųjų transcendentinių skaičių egzistavimo įrodymu.

§99. Algebrinių ir transcendentinių skaičių aibių galios

Ankstesniame paragrafe nustatėme, kad egzistuoja transcendentiniai skaičiai. Todėl realiųjų skaičių aibę $\mathbf{R}$ galime išreikšti dviejų nesikertančių poaibių suma

$$\mathbf{R} = R_a \cup R_t;$$

čia R_a – realiųjų algebrinių skaičių aibė, R_t – realiųjų transcendentinių skaičių aibė. Analogiškai kompleksinių skaičių aibę $\mathbf{K}$ galime išreikšti irgi dviejų nesikertančių poaibių suma

$$\mathbf{K} = K_a \cup K_t,$$

K_a – kompleksinių algebrinių skaičių aibė, K_t – kompleksinių transcendentinių skaičių aibė.

Be to, nustatėme (žr. 185 teoremą ir jos išvadą), kad K_a ir R_a yra laukai.

Realiųjų skaičių aibė nėra suskaičiuojama (žr. 1 d., § 39).

Lema. *Jeigu* $A_1, A_2, \ldots, A_n, \ldots$ *yra baigtinės arba suskaičiuojamos aibės, tai sumos*

$$\bigcup_{i=1}^{\infty} A_i$$

galia ne didesnė už suskaičiuojamos aibės galią.

Įrodymas. Užtenka nagrinėti atvejį, kai aibės poromis neturi bendrų elementų, nes $A \cup B = A \cup (B \setminus A \cap B)$. Antrasis dėmuo turės „daugiausia“ elementų, kai $A \cap B = \varnothing$. Įrodysime, kad tuo atveju, kai aibės poromis neturi bendrų elementų, jų suma yra suskaičiuojama aibė.

Tarkime, kad aibės A_i, $i = 1, 2, \ldots$, yra suskaičiuojamos. Sunumeruosime jų elementus

$$A_i = \{a_{i1}, a_{i2}, a_{i3}, \ldots\}, \quad i = 1, 2, \ldots, n, \ldots$$

Lema bus įrodyta, jei rasime būdą, kaip užrašyti sekos pavidalu sumos

$$\bigcup_{i} A_i$$

elementus.

Tai galime atlikti šitaip: pirmiausia rašome elementą, kurio indeksų suma lygi 2, po to išrašome elementus, kurių indeksų suma lygi 3, toliau –

4, 5 ir t. t. Tuo būdu surašysime visus aibių sumos elementus ir gausime seką. Taigi suma $\bigcup_i A_t$ yra suskaičiuojama.

189 teorema. *Algebrinių skaičių aibė suskaičiuojama.*

Įrodymas. Algebrinių n-ojo laipsnio skaičių aibę žymėsime M_n. Kiekvienas algebrinis n-ojo laipsnio skaičius α yra n-ojo laipsnio polinomo su sveikaisiais koeficientais

$$f(x)=\sum_{k=0}^{n} a_k x^k$$

šaknis. Žymėsime

$$H=\sum_{k=0}^{n} |a_k|$$

ir tą dydį vadinsime algebrinio skaičiaus α aukščiu. Algebrinių n-ojo laipsnio skaičių, kurių aukštis H, yra baigtinis skaičius, nes kiekvienas n-ojo laipsnio polinomas turi n šaknų, o polinomų su sveikaisiais koeficientais ir aukščiu H yra baigtinis skaičius.

Aibę algebrinių n-ojo laipsnio skaičių, kurių aukštis H, žymėsime $M_n^{(H)}$. Ta aibė, kaip įsitikinome, yra baigtinė. Kadangi

$$M_n=\bigcup_{H=1}^{\infty} M_n^{(H)},$$

tai pagal lemą aibės M_n galia ne didesnė už suskaičiuojamos aibės galią.

Visų algebrinių skaičių aibė yra

$$K_a=\bigcup_{n=1}^{\infty} M_n,$$

todėl pagal lemą jos galia ne didesnė už suskaičiuojamos aibės galią. Kadangi aibės K_a galia ne mažesnė už racionaliųjų skaičių aibės galią, tai teorema įrodyta.

Išvada. *Realiųjų algebrinių skaičių aibė yra suskaičiuojama.*

190 teorema. *Realiųjų transcendentinių skaičių aibė nėra suskaičiuojama. Visų transcendentinių skaičių aibė taip pat nėra suskaičiuojama.*

Įrodymas. Įrodysime, kad aibė R_t turi nurodytąją savybę. Tarkime priešingai, R_t yra suskaičiuojama. Kadangi R_t suskaičiuojama, tai pagal lemą aibė

$$\mathbf{R}=R_a \cup R_t$$

taip pat suskaičiuojama. Tai prieštarauja žinomam faktui, kad realiųjų skaičių aibė nėra suskaičiuojama (žr. 1 d., § 39). Taigi prielaida neteisinga. Antrasis teoremos tvirtinimas išplaukia iš to, kad $R_t \subset K_t$.

§100. Apie algebrinių lygčių išsprendžiamumą radikalais

Pagrindinė algebros teorema teigia, kad bet kuris n-ojo laipsnio polinomas su kompleksiniais koeficientais, $n \in \mathbf{N}$, turi n šaknų kompleksinių skaičių lauke. Sunku pervertinti tos teoremos teorinę reikšmę, tačiau praktinė jos reikšmė nedidelė. Ta teorema neteikia jokios informacijos, kaip rasti to ar kito polinomo šaknis konkrečiu atveju. Yra teoremų, kuriose nagrinėjami atskiri polinomų tipai, pateikiami jų šaknų radimo algoritmai, formulės. Vadovėlio 1 dalyje išvedėme antrojo, trečiojo, ketvirtojo laipsnio polinomų ir bet kurio laipsnio dvinarių polinomų šaknų formules. Aptarėme ir kitus tipus polinomų, kurių šaknis galima rasti. Tačiau nepateikėme formulės n-ojo laipsnio bendrojo pavidalo polinomo šaknims rasti. Ar yra tokia formulė? Jeigu jos nėra, tai ar įmanoma kada nors tokią formulę rasti?

Atsakymai į šiuos klausimus ne tokie jau sudėtingi, tačiau juos pagrįsti nėra paprasta. Vadovėlio pirmajame leidime buvo pateikta tokio pagrindimo schema su daugelio atitinkamų tvirtinimų įrodymais. Čia apsiribosime tik bendromis pastabomis.

Iš pradžių aptarsime kai kurias sąvokas bei apibrėžimus.

Radikalais vadiname reiškinius, sudarytus vartojant šaknies ženklą $\sqrt{\ }$ bei kitus aritmetinių veiksmų ženklus, pavyzdžiui, $\sqrt[3]{2}$, $3-\sqrt{5}$ ir pan. Kadangi šaknies traukimo operacija daugiareikšmė, tai konkrečiu atveju reikėtų aptarti, kokias jos reikšmes turėsime mintyje, kalbėdami apie radikalus.

Lygčių išsprendžiamumas priklauso nuo to, kokiame lauke jas nagrinėjame. Tarkime, kad $f(x)$ yra polinomas su sveikaisiais koeficientais. Jeigu jį galime užrašyti sandauga polinomų, kurių kiekvieno laipsnis ne didesnis už 4, tai lygtis

$$f(x)=0,$$

be abejo, išsprendžiama radikalais, t. y. galime parašyti jos šaknų formules, nes žinome 2-ojo, 3-ojo ir 4-ojo laipsnio lygčių šaknų formules. Galime sakyti, kad lygtis išsprendžiama virš racionaliųjų skaičių lauko $\mathbf{Q}$. Tačiau jei polinomas $f(x)$ neišskaidomas virš lauko $\mathbf{Q}$, tai, kai $n \geqslant 5$, tokių formulių neparašysime, nes jų nežinome.

Pereidami prie bendrojo klausimo formulavimo, apibrėšime bendrąją lygtį.

Bendrąja n-ojo laipsnio lygtimi virš lauko $\mathbf{L}$ *vadiname lygtį*

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0; \qquad (11.2)$$

čia $a_1, a_2, \ldots, a_n$ *— nepriklausomi kintamieji, kurie gali įgyti bet kurias lauko* $\mathbf{L}$ *elementų reikšmes.*

Pavyzdžiui, lygtį $x^2+ax+b=0$, kai a ir b — bet kurie racionalieji skaičiai, vadiname bendrąja 2-ojo laipsnio lygtimi virš lauko $\mathbf{Q}$.

Suformuluosime vieną iš galimų lygčių išsprendžiamumo radikalais apibrėžimų.

Bendroji n-ojo laipsnio lygtis

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

virš skaičių lauko **L** *išsprendžiama radikalais, jeigu yra tokia formulė*

$$R(a_1, a_2, \ldots, a_n),$$

turinti, be 4 *aritmetinių veiksmų ženklų, tik ženklą* $\sqrt{\ }$, *kad su bet kuriuo rinkiniu*

$$a_1^0, a_2^0, \ldots, a_n^0 \in \mathbf{L}$$

reiškinys

$$R(a_1^0, a_2^0, \ldots, a_n^0)$$

yra (konkrečios) lygties

$$x^n + a_1^0 x^{n-1} + \ldots + a_n^0 = 0$$

šaknis.

Į formulę R gali įeiti ir kai kurios konstantos $c \in \mathbf{L}$. Šis apibrėžimas, nežiūrint jo bendrumo, turi vieną trūkumą – jis nėra konstruktyvus. Todėl pateiksime ir kitą apibrėžimą, kuris, be kita ko, labiau siesis ir su kitais toliau nagrinėjamais klausimais.

Paprastuoju dvinariu plėtiniu pavadinkime lauko **L** *plėtinį* **L** (α, ζ), kai α yra dvinarės lygties

$$x^n - a = 0$$

$(a \in L,\ a \neq 0)$ šaknis, o ζ – primityvioji n-ojo laipsnio vieneto šaknis.

P vadinamas *dvinariu lauku* **L** *plėtiniu*, jei jis gaunamas sudarant grandinę paprastųjų dvinarių lauko **L** plėtinių, t. y. jei su visais i $(1 \leqslant i \leqslant s)$ laukas $\mathbf{L}_i$ yra paprastasis dvinaris lauko $\mathbf{L}_{i-1}$ plėtinys:

$$\mathbf{L} = \mathbf{L}_0 \subset \mathbf{L}_1 \subset \ldots \subset \mathbf{L}_{s-1} \subset \mathbf{L}_s = \mathbf{P}.$$

Sakoma, kad polinomo virš lauko **L** *šaknis išreiškiama radikalais, jei egzistuoja dvinaris lauko* **L** *plėtinys, kuriam priklauso ta šaknis.*

Vadinasi, jeigu polinomo $f(x)$ šaknis α išreiškiama radikalais, tai jos radimas pakeičiamas nuosekliu tam tikro skaičiaus dvinarių lygčių sprendimu.

Lygtis

$$f(x)=0$$

išsprendžiama radikalais, jei visos polinomo $f(x)$ *šaknys išreiškiamos radikalais.*

Nemažai matematikų nagrinėjo (11.2) pavidalo algebrinių lygčių išsprendžiamumo radikalais problemą. 1798 m. italas *P. Rufinis* (P. Ruffini, 1765–1822) mėgino įrodyti, kad aukštesnio negu ketvirtojo laipsnio bendroji lygtis radikalais neišsprendžiama.

Norvegų matematikas *N. Abelis* (N. Abel, 1802–1829) įrodė, kad nėra universalios formulės, išreiškiančios (11.2) lygties sprendinius, kai $n \geqslant 5$.

Pateiksime be įrodymo Abelio teoremą.

191 (Abelio) teorema. *Bendrojo pavidalo*

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

algebrinė lygtis virš bet kokio lauko **L**, *kai* $n \geqslant 5$, *neišsprendžiama radikalais.*

Iš Abelio teoremos neišplaukia, kad nėra išsprendžiama radikalais (11.2) pavidalo lygtis su konkrečiais koeficientais. Pavyzdžiui, lygtys $x^{10}-7x^5+2=0$ ir $x^6-3=0$ išsprendžiamos radikalais. Tačiau lygtis $x^5+7x+7=0$ neišsprendžiama radikalais.

Išsamų atsakymą į tą klausimą randame anksti žuvusio talentingo prancūzų matematiko *Evaristo Galua* (E. Galois, 1811–1832) darbuose. Jis nagrinėjo algebrinių lygčių išsprendžiamumo radikalais klausimą ir įrodė, kad egzistuoja konkrečios aukštesnio negu ketvirtojo laipsnio lygtys, kurios neišsprendžiamos radikalais. Lygčių išsprendžiamumas radikalais Galua teorijoje siejamas su tam tikros, tai lygčiai priskirtos grupės (*Galua grupės*) savybėmis.

Paminėsime vieną teiginį, išplaukiantį iš Galua teorijos.

Jeigu p *yra pirminis skaičius, tai 5-ojo laipsnio lygtis*

$$x^5+px+p=0$$

racionaliųjų skaičių lauke neišsprendžiama radikalais.

Trumpai aptarsime 3-ojo ir 4-ojo laipsnio lygčių išsprendžiamumą antrojo laipsnio (kvadratiniais) radikalais.

§101. Kubinių lygčių išsprendžiamumas kvadratiniais radikalais

Lygtis išsprendžiama kvadratiniais radikalais, jeigu jos sprendiniams rasti egzistuoja formulės, į kurias, be keturių aritmetinių operacijų ženklų, įeina kvadratinės šaknies traukimo ženklas, lygties koeficientai ir lauko **L**, virš kurio nagrinėjama lygtis, skaičiai.

192 teorema. *Jeigu viena kubinės lygties su kompleksiniais koeficientais*

$$f(x)=x^3+a_2x^2+a_1x+a_0=0$$

šaknis x_1 išreiškiama kvadratiniais radikalais, tai jais išreiškiamos ir kitos šaknys.

Įrodymas. Tarkime, kad x_1 yra lygties $f(x)=0$ šaknis. Iš išraiškos

$$f(x)=(x-x_1)(x^2+px+q),$$

naudodamiesi Hornerio schema, gauname

$$p=x_1+a_2,$$

$$q=x_1^2+a_2x_1+a_1.$$

Išsprendę kvadratinę lygtį $x^2+px+q=0$, randame kitas dvi polinomo $f(x)$ šaknis:

$$x_{2,3}=-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}.$$

Aišku, jei x_1, tai ir skaičiai p, q išreiškiami polinomo $f(x)$ koeficientais ir kvadratiniais radikalais. Iš pastarosios lygybės matome, kad tas tvirtinimas teisingas ir šaknims x_2 bei x_3. Teorema įrodyta.

Lauką, kuris gaunamas prie racionaliųjų skaičių lauko Q prijungus polinomo

$$g(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1+a_0$$

koeficientus, vadinsime lygties

$$g(x)=0$$

racionalumo sritimi ir žymėsime $\mathbf{F}=Q(a_n, \ldots, a_1, a_0)$.

193 teorema. *Kubinė lygtis*

$$f(x)=x^3+a_2x^2+a_1x+a_0=0 \qquad (11.3)$$

su kompleksiniais koeficientais išsprendžiama kvadratiniais radikalais tada ir tik tada, kai ji turi bent vieną šaknį savo racionalumo srityje **F**.

Įrodymas. Sąlygos pakankamumas akivaizdus. Iš tikrųjų, jeigu polinomas $f(x)$ turi šaknį x_1 racionalumo srityje **F**, tai virš **F** jis užrašomas sandauga

$$f(x)=(x-x_1)(x^2+px+q)=0$$

ir išsprendžiamas radikalais.

Būtinumas. Tarkime, kad (11.3) lygtis išsprendžiama kvadratiniais radikalais, tačiau ji neturi šaknų savo racionalumo srityje **F**.

Atlikdami aritmetines operacijas su lygties racionalumo srities **F** skaičiais, vėl gauname lauko **F** skaičius. Kvadratinės šaknies traukimo iš lauko **F** skai-

čiaus α operacijos rezultatas gali būti lauko $\mathbf{F}$ skaičius (jei α yra lauko $\mathbf{F}$ skaičiaus kvadratas) arba lauko $\mathbf{F}$ kvadratinio plėtinio skaičius. Pažymėsime

$$\mathbf{F}_1=\mathbf{F}(\sqrt{\alpha});$$

čia $\alpha\in F$, bet nėra kvadratas lauke $\mathbf{F}$.

Atlikdami keturias aritmetines operacijas su lauko $\mathbf{F}$ skaičiais, vėl gausime lauko $\mathbf{F}$ skaičius. Tačiau traukdami kvadratinę šaknį iš lauko $\mathbf{F}_1$ skaičiaus α_1, kuris nėra kvadratas tame lauke, gausime skaičių, priklausantį lauko $\mathbf{F}_1$ kvadratiniam plėtiniui $\mathbf{F}_2$:

$$\mathbf{F}_2=\mathbf{F}_1(\sqrt{\alpha_1}).$$

Taigi jeigu, sprendžiant (11.3) lygtį kvadratiniais radikalais, tenka m kartų traukti kvadratinę šaknį ir atlikti sudėties, atimties, dalybos bei daugybos operacijas, tai visų tų veiksmų rezultatas priklauso laukui $\mathbf{F}_k$, gautam iš lauko $\mathbf{F}$, nuosekliai atlikus k kvadratinių plėtinių:

$$\begin{aligned}
&\mathbf{F}_1=\mathbf{F}(\sqrt{\alpha}), && \alpha\in\mathbf{F},\\
&\mathbf{F}_2=\mathbf{F}_1(\sqrt{\alpha_1}), && \alpha_1\in\mathbf{F}_1,\\
&\mathbf{F}_3=\mathbf{F}_2(\sqrt{\alpha_2}), && \alpha_2\in\mathbf{F}_2,\\
&\cdots\cdots\cdots && \cdots\cdots\\
&\mathbf{F}_k=\mathbf{F}_{k-1}(\sqrt{\alpha_{k-1}}), && \alpha_{k-1}\in\mathbf{F}_{k-1}.
\end{aligned} \tag{11.4}$$

Jeigu nė vienas iš skaičių α, α_1, ..., α_{k-1} nėra kvadratas atitinkamuose laukuose, tai $m=k$, priešingu atveju $m>k$.

Tarkime, kad, priešingai teoremos tvirtinimui, nė viena (11.4) lygties šaknis nepriklauso lygties racionalumo sričiai $\mathbf{F}$. Visos šaknys, kurios išreiškiamos kvadratiniais radikalais, priklauso lauko $\mathbf{F}$ kvadratinių plėtinių (11.4) sekos laukams $\mathbf{F}_l$. Tarkime, kad k – toks mažiausias numeris, kad bent viena (11.3) lygties šaknis x_1 priklauso laukui $\mathbf{F}_k$. Kitos tos lygties šaknys priklauso arba laukui $\mathbf{F}_k$, arba didesnio indekso lauko $\mathbf{F}$ plėtiniui $\mathbf{F}_l$, $l>k$. Taigi nėra nė vienos tos lygties šaknies, kuri priklausytų plėtiniui $\mathbf{F}_{k-1}$.

Kiekvieną lauko $\mathbf{F}_{k-1}$ kvadratinio plėtinio $\mathbf{F}_k$ skaičių, taigi ir skaičių x_1, galima užrašyti šitaip:

$$x_1=b+c\sqrt{d};$$

čia b, c, $d\in\mathbf{F}_{k-1}$, d nėra kvadratas lauke $\mathbf{F}_{k-1}$. Vadinasi,

$$\sqrt{d}\notin\mathbf{F}_{k-1}.$$

Skaičius x_1 yra polinomo $f(x)$ šaknis, tada

$$\begin{aligned}
f(x_1)&=x_1^3+a_2x_1^2+a_1x_1+a_0=(b+c\sqrt{d})^3+\\
&+a_2(b+c\sqrt{d})^2+a_1(b+c\sqrt{d})+a_0=\\
&=b^3+3bc^2d+a_2b^2+a_2c^2d+a_0+(3b^2c+cd+2a_2bc+a_1c)\sqrt{d}=\\
&=G_1+G_2\sqrt{d}=0.
\end{aligned}$$

Kadangi (11.3) lygties koeficientai yra lauko $\mathbf{F}$, kartu ir lauko $\mathbf{F}_{k-1}$ skaičiai, b, c, d taip pat priklauso laukui $\mathbf{F}_{k-1}$, tai

$$G_1 = b^3 + 3bc^2 d + a_2 b^2 + a_2 c^2 d + a_0 \in \mathbf{F}_{k-1},$$

$$G_2 = 3b^2 c + cd + 2a_2 bc + a_1 c \in \mathbf{F}_{k-1}.$$

Jeigu $G_2 \neq 0$, tai

$$f(x_1) = 0 \Rightarrow G_1 + G_2 \sqrt{d} = 0 \Rightarrow \sqrt{d} = -\frac{G_1}{G_2} \Rightarrow \sqrt{d} \in \mathbf{F}_{k-1},$$

bet tai prieštarauja prielaidai, kad $\sqrt{d} \in \mathbf{F}_{k-1}$. Vadinasi, G_2, kartu ir G_1, yra lygūs 0:

$$G_1 = G_2 = 0.$$

Tačiau iš paprastų skaičiavimų išplaukia

$$f(b - c\sqrt{d}) = G_1 - G_2 \sqrt{d} = 0.$$

Vadinasi, jeigu $x_1 = b + c\sqrt{d}$ yra viena (11.3) lygties šaknis, tai kita šaknis yra

$$x_2 = b - c\sqrt{d}.$$

Tuo atveju polinomas $f(x)$ dalijasi iš sandaugos

$$h(x) = (x - x_1)(x - x_2) = (x - b)^2 - dc^2.$$

Tačiau polinomo $h(x)$ koeficientai priklauso laukui F_{k-1}, taigi polinomas $f(x)$ lauke $\mathbf{F}_{k-1}$ išskaidomas:

$$f(x) = h(x)(x - x_3) = \left((x - b)^2 - dc^2\right)(x - x_3)$$

ir todėl $x_3 \in \mathbf{F}_{k-1}$.

Kadangi x_3 yra (11.3) lygties šaknis, tai ji negali priklausyti laukui $\mathbf{F}_{k-1}$ pagal skaičiaus k apibrėžimą. Iš gautojo prieštaravimo išplaukia, kad prielaida yra neteisinga, t. y. bent viena (11.3) lygties šaknis priklauso laukui $\mathbf{F}$.

1 išvada. *Trečiojo laipsnio algebrinė lygtis su racionaliaisiais koeficientais, neturinti racionaliųjų šaknų, kvadratiniais radikalais neišsprendžiama.*

Įrodymas. Šiuo atveju (11.3) lygties racionalumo sritis $\mathbf{F}$ sutampa su racionaliųjų skaičių lauku $\mathbf{Q}$.

2 išvada. *Ketvirtojo laipsnio algebrinė lygtis*

$$x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0 \qquad (11.5)$$

yra išsprendžiama kvadratiniais radikalais tada ir tik tada, kai jos rezolventė turi bent vieną šaknį savo racionalumo srityje.

Įrodymas. Keitiniu $y = x + (a_3/4)$ iš (11.5) lygties gauname lygtį

$$y^4 + 2py^2 + qy + r = 0, \qquad (11.6)$$

kurios rezolventė yra lygtis

$$64z^3+64pz^2-16(r-p^2)z-q^2=0. \qquad (11.7)$$

I dalyje įsitikinome, kad (11.6) ir (11.7) lygčių šaknys y_0 ir z_0 susietos lygybėmis

$$y_0^2 \pm 2\sqrt{z_0}y_0+\left(p+2z_0 \pm \frac{q}{4\sqrt{z_0}}\right)=0.$$

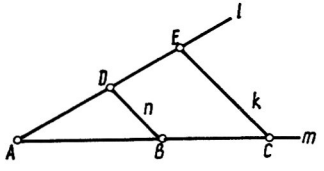
Todėl y_0 ir z_0 kartu yra išreiškiamos arba neišreiškiamos kvadratiniais radikalais.

§102. Brėžimas skriestuvu ir liniuote

Brėžimo uždaviniai visada buvo vieni iš labiausiai mėgstamų geometrijos uždavinių. Matematikos istorijoje ypatingą vietą užima *brėžimo tik skriestuvu ir liniuote* uždaviniai.

Liniuotė, kuria galima naudotis tuose uždaviniuose, turi būti be padalų. Vadinasi, ja naudodamiesi, galime nubrėžti tik tiesias linijas, negalime atidėti atkarpų nei jų išmatuoti. Skriestuvu galime brėžti bet kokio spindulio apskritimus.

Brėžimo skriestuvu ir liniuote uždaviniai ir paprasti, ir sudėtingi. Yra ir tokių uždavinių, kurių sprendinio šimtmečiais veltui ieškojo matematikai. Paaiškėjo, kad, naudojantis tik skriestuvu ir liniuote, atkarpą AB galima nubrėžti tik tada, kai tos atkarpos ilgis yra algebrinis skaičius. Jeigu pradinėse uždavinio sąlygose figūruoja atkarpos, kurių ilgis — racionalusis skaičius, tai, naudojantis tik skriestuvu ir liniuote, negalima nubrėžti atkarpos, kurios ilgis būtų transcendentinis skaičius. Tačiau toji būtina sąlyga nėra pakankama, nes ne visi algebriniai skaičiai yra skriestuvu ir liniuote nubrėžiamų atkarpų ilgiai.



3 pav.

Analizinis brėžimo skriestuvu ir liniuote uždavinių nagrinėjimas glaudžiai siejasi su Galua teorija.

Iš pradžių nagrinėsime paprasčiausias operacijas, kurias galima atlikti su atkarpomis skriestuvu ir liniuote.

Visiems gerai žinoma, kaip sudėti ir atimti atkarpas. Priminsime atkarpų daugybos ir dalybos būdus. Tarkime, kad turime dvi atkarpas, kurių ilgiai yra a ir b. Atkarpų, kurių ilgiai būtų lygūs ab ir $\frac{b}{a}$, brėžimas pavaizduotas 3 paveiksle.

Visuose brėžimo uždaviniuose laikysime, kad vienetinės atkarpos ilgis lygus 1.

Brėždami atkarpą, kurios ilgis lygus ab, a ir b — dviejų žinomų atkarpų ilgiai, liniuote brėžiame dvi smailiuoju kampu susikertančias tieses l ir m. Vienoje jų, pavyzdžiui, tiesėje l, skriestuvu atidedame vienetinę atkarpą AD ir atkarpą AE, kurios ilgis lygus skaičiui a. (Paveiksle atvaizduotas atvejis, kai $a>1$. Padarius atitinkamus pakeitimus, uždavinys nesunkiai sprendžiamas ir tuo atveju, kai $a<1$.) Tiesėje m atidedame atkarpą AB, kurios ilgis

lygus b. Taškus D ir B sujungiame tiese n. Iš taško E išvedame tiesę k, lygiagrečią tiesei n, kuri taške C kerta tiesę m. Iš trikampių ADB ir AEC panašumo gauname

$$AD : AB = AE : AC,$$

arba

$$AC = \frac{AB \cdot AE}{AD}.$$

Akivaizdu, kad atkarpos AC ilgis lygus ab.

Norėdami nubrėžti atkarpą, kurios ilgis būtų $\frac{1}{a}$, $a<1$, turime nubrėžti vienetines atkarpas AB, AE ir a ilgio atkarpą AD (žr. 3 pav.). Jei $a>1$, atitinkamai sukeistume D ir E.

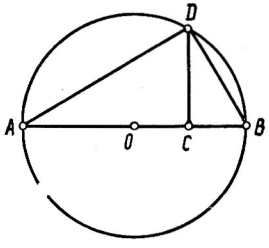
Dabar galime nubrėžti ir atkarpą, kurios ilgis būtų dviejų atkarpų a ir b santykis. Iš tikrųjų pakanka remtis tuo, kad

$$\frac{a}{b} = a \cdot \frac{1}{b}.$$

Įrodysime teoremą.

194 teorema. *Jeigu duota vienetinė atkarpa, tai skriestuvu ir liniuote galima nubrėžti visus racionaliųjų skaičių lauko* **Q** *skaičius vaizduojančias atkarpas.*

Įrodymas. Turint vienetinę atkarpą, galima nubrėžti atkarpą, kurios ilgis būtų $1+1=2$. Turint atkarpas, kurių ilgiai yra 1 ir 2, galima nubrėžti atkarpą, kurios ilgis būtų $1+2=3$ ir t. t. Akivaizdu, kad iš principo (t. y. atsiribojant nuo praktinių galimybių, kurias sąlygoja laikas, popieriaus ar kitos medžiagos atsargos ir pan.) galima nubrėžti bet kurį natūrinį skaičių vaizduojančią atkarpą. Kadangi bet kurį teigiamą racionalųjį skaičių $\frac{a}{b}$ galima išreikšti dviejų natūrinių skaičių a ir b santykiu, tai skriestuvu ir liniuote galima nubrėžti ir visas atkarpas, kurių ilgis yra racionalusis skaičius. Neigiamus racionaliuosius skaičius vaizduos to paties ilgio atkarpos, kurios vaizduoja atitinkamus teigiamuosius skaičius, tik joms priskiriama priešinga kryptis.



4 pav.

Toliau trumpumo dėlei vietoj „nubrėžti a ilgio atkarpą“ sakysime „nubrėžti (skaičių) a“.

195 teorema. *Jeigu skriestuvu ir liniuote galima nubrėžti visus lauko* **L** *skaičius, tai galima nubrėžti ir visus lauko* **L** *kvadratinio plėtinio* $\mathbf{F}=\mathbf{L}(\sqrt{q})$, $q>0$, $q \in \mathbf{L}$, *skaičius.*

Įrodymas. Pakanka nagrinėti atvejį, kai $\sqrt{q}\in L$. Žinome, kad bet kuris lauko $\mathbf{F}$ skaičius yra

$$a+b\sqrt{q}$$

pavidalo; čia a, b, $q\in L$. Kadangi nubrėžiamų skriestuvu ir liniuote skaičių suma ir sandauga taip pat nubrėžiamos tomis priemonėmis, tai pakanka įrodyti, kad, mokant nubrėžti skriestuvu ir liniuote skaičių q, galima nubrėžti ir skaičių $\sqrt{q}$.

Nubrėžiame $q+1$ skersmens apskritimą. Jo skersmenyje AB taip pažymime tašką C, kad atkarpos AC ilgis būtų lygus q. Tuomet atkarpos CB ilgis lygus 1. Iš taško C iškeliame statmenį (skriestuvu ir liniuote), kuris kerta apskritimą taške D. Iš žinomų apskritimo savybių išplaukia, kad

$$AC:CD=CD:CB,$$

t. y.

$$CD^2=AC\cdot CB.$$

Akivaizdu, kad atkarpos CD ilgis lygus $\sqrt{q}$. Taigi, jeigu q, tai ir $\sqrt{q}$ nubrėžiama skriestuvu ir liniuote.

§103. Pagrindinė brėžimo skriestuvu ir liniuote teorema

Šiame paragrafe įrodysime teoremą, kuri nusako klasę skaičių, nubrėžiamų skriestuvu ir liniuote.

196 teorema. *Būtina ir pakankama sąlyga, kad realųjį skaičių* ω *būtų galima nubrėžti skriestuvu ir liniuote – kad* ω *turi priklausyti racionaliųjų skaičių lauko* $\mathbf{Q}=\mathbf{F}=\mathbf{F}_0$ *kvadratinių plėtinių sekos* (11.4) *laukui* $\mathbf{F}_k$.

Įrodymas. Sąlygos pakankamumas aiškus. Iš tikrųjų, jeigu $\mathbf{F}_k$ – vienas iš (11.4) sekos laukų, tai iš 194 ir 195 teoremų išplaukia, kad skaičių ω, kaip ir visus lauko $\mathbf{F}_k$ skaičius, galima nubrėžti skriestuvu ir liniuote.

Įrodysime sąlygos būtinumą. Skriestuvu ir liniuote brėždami tik apskritimus ir tieses, gauname trejopus susikirtimo taškus: dviejų tiesių, tiesės ir apskritimo, dviejų apskritimų.

Plokštumoje įveskime koordinačių sistemą. Dviejų tiesių, atitinkamai nubrėžtų per taškus $\alpha_1(x_1, y_1)$, $\alpha_2(x_2, y_2)$ ir $\beta_1(u_1, v_1)$, $\beta_2(u_2, v_2)$, lygtys yra

$$\frac{x-x_1}{x_2-x_1}=\frac{y-y_1}{y_2-y_1},$$

$$\frac{x-u_1}{u_2-u_1}=\frac{y-v_1}{v_2-v_1}.$$

Tų dviejų tiesių susikirtimo taškas γ randamas sprendžiant dviejų tiesinių lygčių sistemą. Taigi taško γ koordinatės gaunamos atliekant keturias aritmetines operacijas su sistemos koeficientais ir racionaliaisiais skaičiais. Jeigu

taškų α_1, α_2, β_1, β_2 koordinatės priklauso kuriam nors laukui **L**, tai tam pačiam laukui priklauso ir taško γ koordinatės. Vadinasi, brėždami tieses liniuote, iš taškų su laukui **L** priklausančiomis koordinatėmis gauname taškus, kurių koordinatės irgi priklauso laukui **L**.

Kaip žinome, atkarpos, jungiančios taškus α (x, y) ir β (u, v), ilgis išreiškiamas formule

$$d=\sqrt{(u-x)^2+(v-y)^2}.$$

Jeigu taškų α ir β koordinatės priklauso laukui **L**, tai tuos taškus jungiančios atkarpos ilgis d gali nepriklausyti laukui **L**, tada jis priklauso kuriam nors kvadratiniam lauko **L** plėtiniui. Taigi, naudodamiesi liniuote, iš taškų su koordinatėmis, priklausančiomis laukui **L**, ir atkarpų, kurių ilgiai yra lauko **L** skaičiai, gauname taškus ir atkarpas, kurių koordinatės bei ilgiai atitinkamai priklauso lauko **L** nuoseklių kvadratinių plėtinių sekos laukams.

Dviejų apskritimų, kurių centrai — taškai α_1, α_2, o spinduliai — r_1 ir r_2, lygtys yra

$$(x-x_1)^2+(y-y_1)^2=r_1^2, \tag{11.8}$$

$$(x-x_2)^2+(y-y_2)^2=r_2^2. \tag{11.9}$$

Ieškant tų apskritimų susikirtimo taško, tenka spręsti tų dviejų lygčių sistemą. Iš (11.8) lygties panariui atėmę (11.9) lygtį, turime

$$(2x-x_1-x_2)(x_2-x_1)+(2y-y_1-y_2)(y_2-y_1)=r_1^2-r_2^2.$$

Ši lygtis reiškia tiesę, nubrėžtą per dviejų apskritimų (11.8) ir (11.9) susikirtimo taškus. Tų susikirtimo taškų koordinates randame spręsdami dviejų lygčių sistemą: viena tos sistemos lygtis yra užrašytoji tiesės lygtis, kita — bet kuri iš (11.8) ir (11.9) lygčių. Iš tokios sistemos gauname vieno kintamojo kvadratinę lygtį.

Taigi, naudodamiesi tik skriestuvu, iš taškų, kurių koordinatės yra lauko **L** skaičiai, ir atkarpų, kurių ilgiai taip pat yra lauko **L** skaičiai, vėl gauname taškus ir atkarpas, kurių koordinatės bei ilgiai yra skaičiai, priklausantys lauko **L** kvadratinių plėtinių sekos laukams.

Akivaizdu, kad tą patį rezultatą gauname ir naudodamiesi liniuote ir skriestuvu kartu.

Įrodėme (194 teorema), kad turėdami vienetinę atkarpą galime nubrėžti visus racionaliųjų skaičių lauko **Q** skaičius. Todėl galime imti $\mathbf{F}=\mathbf{F}_0=\mathbf{Q}$. Iš tos teoremos įrodymo išplaukia, kad visi skaičiai, kuriuos galima nubrėžti skriestuvu ir liniuote, priklauso lauko **Q** kvadratinių plėtinių (11.4) sekai (savaime aišku, kalbama tik apie realiuosius plėtinius $\mathbf{F}_m(\sqrt{\alpha_m})$, $\alpha_m>0$).

§104. Keturių klasikinių brėžimo uždavinių neišsprendžiamumas

Kai kurie brėžimo skriestuvu ir liniuote uždaviniai turi ilgą nesėkmingų sprendinio ieškojimų istoriją. Prie tokių uždavinių priklauso ir keli klasikiniai. Juos čia ir nagrinėsime.

Kubo dvigubinimas. *Ar galima skriestuvu ir liniuote nubrėžti kubą, kurio tūris būtų dvigubai didesnis už pradinio kubo tūrį?*

Norint išspręsti uždavinį, reikia mokėti nubrėžti naujojo kubo briauną x, kai žinoma pradinio kubo briauna, kurią galima laikyti lygia 1. Iš sąlygos turime

$$x^3 = 2.$$

Taigi reikia mokėti nubrėžti tos kubinės lygties šaknį. Tačiau nesunku įsitikinti, kad lygtis

$$x^3 - 2 = 0$$

racionaliųjų šaknų neturi, nes visos galimos tokios lygties racionaliosios šaknys yra sveikieji skaičiai, laisvojo nario dalikliai: ± 1, ± 2.

Tačiau tie sveikieji skaičiai nėra šios lygties šaknys. Pagal 193 teoremos išvadą ta lygtis neišsprendžiama kvadratiniais radikalais, todėl pagal 196 teoremą lygties $x^3 - 2 = 0$ šaknis negali būti nubrėžta naudojantis tik skriestuvu ir liniuote.

Kampo trisekcija. *Ar galima skriestuvu ir liniuote bet kurį kampą padalyti į 3 lygias dalis?*

Akivaizdu, kad reikiamą kampą φ nubrėšime, jei galime nubrėžti to kampo trigonometrinių funkcijų reikšmes, ir atvirkščiai. Yra kampų, kuriuos galima dalyti į 3 dalis, pavyzdžiui, 90°, 180° ir kt. Įrodysime, kad yra bent vienas kampas, kurio negalima padalyti į tris dalis skriestuvu ir liniuote. Toks kampas, pavyzdžiui, yra 60°. Nagrinėsime, ar galima nubrėžti $x = \cos 20°$. Kadangi

$$\cos \varphi = 4 \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3},$$

tai skaičius x yra lygties

$$\cos 60° = 4x^3 - 3x$$

šaknis. Tą lygtį galime užrašyti šitaip:

$$8x^3 - 6x - 1 = 0.$$

Pažymėję $2x = y$, turime

$$y^3 - 3y - 1 = 0.$$

Panašiai kaip ir ankstesniu atveju nustatome, kad pastaroji lygtis neturi racionaliųjų šaknų, todėl ji neišsprendžiama kvadratiniais radikalais. Vadinasi, skaičiaus y, kartu ir x *negalima nubrėžti* naudojantis tik skriestuvu ir liniuote.

Skritulio kvadratūra. *Ar galima nubrėžti kvadratą, kurio plotas būtų lygus skritulio plotui?*

Jeigu skritulio spindulys lygus vienetui, tai ieškomojo kvadrato kraštinė yra lygties

$$x^2 = \pi$$

šaknis. Ar galima skriestuvu ir liniuote nubrėžti tos lygties šaknį $\sqrt{\pi}$? Jeigu galima nubrėžti $\sqrt{\pi}$, tai galima nubrėžti ir skaičių π, ir atvirkščiai. Tačiau, norint nubrėžti skaičių π, reikia žinoti jo reikšmę.

Ilgą laiką buvo ieškoma „tikslios" skaičiaus π išraiškos brėžiant vis didesnį kraštinių skaičių turinčius daugiakampius. 1579 m. *F. Vietas*, pritaikęs Archimedo būdą 393216-kampiui, rado 10 tikslių skaičiaus π dešimtainių skaitmenų. Netrukus flamandų matematikas *A. Romenas*, naudodamasis 1073741824-kampiu, apskaičiavo 15 skaičiaus π dešimtainių skaitmenų. Trejais metais vėliau *Liudolfas van Kiolenas*, naudodamasis daugiau kaip 32 milijardus kraštinių turinčiu daugiakampiu, 1596 m. rado 20 tikslių skaičiaus π skaitmenų. Po jo mirties užrašuose buvo apskaičiuota dar 15 skaičiaus π skaitmenų. Tie skaitmenys, matyt, buvo labai brangūs Kiolenui, nes jis prašė iškalti juos antkapyje. Pagerbiant tą žymų skaičiuotoją, skaičius π kurį laiką buvo vadinamas *Liudolfo skaičiumi.*

Tačiau net 35 skaitmenys po kablelio neatskleidė skaičiaus π prigimties. O skritulio kvadratūros uždavinio sprendėjų skaičius augo, klaidingais sprendimais buvo užverstos mokslo įstaigos ir akademijos. Tos problemos sprendėjus imta vadinti *kvadratūristais.* 1775 m. Paryžiaus akademija nusprendė daugiau nepriimti darbų apie skritulio kvadratūrą,nors tuos darbus tikrinusi komisija nebuvo likviduota; ją pavadino „Prapuolusių vaikų komisija".

1882 m. F. Lindemanas įrodė, kad skaičius π yra transcendentinis. Iš 196 teoremos išplaukia, kad π, kaip nealgebrinis skaičius, negali būti nubrėžtas naudojantis tik skriestuvu ir liniuote.

Taisyklingasis septynkampis. *Ar galima įbrėžti į apskritimą taisyklingąjį septynkampį?*

Pakanka rasti tokio septynkampio kraštinę x. Apskritimo spindulį galime laikyti lygiu vienetui. Jeigu nubrėšime vienetinį apskritimą kompleksinėje plokštumoje, centru parinksime koordinačių pradžią, viena septynkampio viršūne laikysime tašką (1, 0), tai kitos to daugiakampio viršūnės bus tie skaičiai z, kurie tenkina lygtį

$$z^7 = 1.$$

Padaliję tą lygtį iš $z-1$, gauname

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0.$$

Padaliję iš z^3, gauname lygtį

$$\left(z + \frac{1}{z}\right)^3 - 3\left(z + \frac{1}{z}\right) + \left(z + \frac{1}{z}\right)^2 - 1 + \left(z + \frac{1}{z}\right) = 0.$$

Po keitinio

$$z + \frac{1}{z} = y$$

turime kubinę lygtį

$$y^3 + y^2 - 2y - 1 = 0.$$

Tos lygties racionaliosios šaknys gali būti tik sveikieji skaičiai, lygties laisvojo nario dalikliai ± 1, tačiau akivaizdu, kad tie skaičiai nėra šaknys. Vadinasi, lygtis racionaliųjų šaknų neturi, todėl ji neišsprendžiama kvadratiniais radikalais. Kadangi z ir y kartu išreiškiami arba neišreiškiami kvadrati-

niais radikalais, tai iš čia išplaukia, kad taškai z – taisyklingojo septynkampio viršūnės – negali būti randami naudojantis tik skriestuvu ir liniuote. Taigi ir tas uždavinys *neišsprendžiamas*.

Įrodėme, kad šios 4 brėžimo problemos galutinai išspręstos. Deja, garsas apie jas pasklido žymiai plačiau negu žinios apie jų išsprendimą. Daugybė matematikos mėgėjų veltui plušo mėgindami sukonstruoti vieno ar kito uždavinio brėžimo schemą. Deja, tokių sprendėjų esama ir dabar. Matematikos mokytojams gali tekti su jais susidurti. Tikimės, kad šiame paragrafe pateikti įrodymai padės išaiškinti tokių darbų beprasmiškumą.

Kalbant apie šias pagarsėjusias problemas, tikslinga paminėti dar vieną, galbūt pačią garsiausią problemą. Tai vadinamoji *Ferma problema*. Šiai problemai bei vienai kitai lygčiai aptarti ir skirsime paskutinį vadovėlio paragrafą.

§105. Aukštesniojo laipsnio Diofanto lygtys

Pirmojo laipsnio dviejų ar daugiau kintamųjų Diofanto lygtis jau esame aptarę. Jų sprendimas aiškus, nors kartais gali būti ir ilgokas. Tokios lygtys arba visai neturi sprendinių, arba jų turi be galo daug.

Aukštesniojo laipsnio Diofanto lygčių sprendimas žymiai komplikuotesnis. Vieno tipo lygtis mokame spręsti, kito tipo – ne. Neperdedant galima pasakyti, kad kiekviena aukštesniojo laipsnio Diofanto lygtis – atskira problema.

Viena iš labiausiai žinomų Diofanto lygčių – tai *Ferma lygtis*

$$x^n + y^n = z^n.$$

Keletas žodžių apie Diofantą. Nedaug žinių apie šį matematiką mus pasiekė iš amžių gilumos. Nežinome, nei kada jis gimė, nei kada mirė. Iš kai kurių duomenų spėjama, kad jis galėjo gyventi apie 250 mūsų eros metus. Iš vienos jam skirtos eiliuotos aritmetinio uždavinio formos epigramos aiškėja, kad jis pragyvenęs 84 metus. Ne visos Diofanto parašytos knygos pasiekė mūsų laikus – iš 13 jo „Aritmetikos“ knygų išliko tik 6. Laikas nuo laiko išlikusios jo knygos buvo perspausdinamos (pirmasis ir kol kas paskutinis jo „Aritmetikos“ leidimas Tarybų Sąjungoje išėjo rusų kalba 1974 m. Maskvoje).

Prancūzų matematikas P. Ferma, kurį jau ne kartą minėjome (beje, tikroji jo profesija – juristas), nagrinėdamas Diofanto knygoje pateiktą lygtį, knygos paraštėje parašė: „Nei kubas į du kubus, nei kvadrato kvadratas ir apskritai, išskyrus kvadratą, joks laipsnis negali būti išdėstytas tokių pat dviejų laipsnių suma. Aš radau nuostabų tos hipotezės įrodymą, bet per siauros paraštės neleidžia jo išdėstyti“.

P. Ferma sūnus po tėvo mirties išspausdino Diofanto knygą kartu su visomis tėvo pastabomis. Paprasta iškelto uždavinio formuluotė, masinanti Ferma pastaba apie nuostabaus įrodymo galimybę sudomino ne vieną. Lygtį $x^n + y^n = z^n$ imta vadinti *Ferma lygtimi*, jos sprendimo problemą – *Ferma problema*, arba kitaip – *didžiąja Ferma teorema*. Ferma problemos sprendėjų gretos keleriopai pagausėjo, 1908 m. matematinėje spaudoje paskelbus Getingeno „Karališkosios mokslo draugijos“ statutą apie matematiko *Pauliaus Volfskelio* palikimą. Jis paskyrė 100 000 vokiškų markių tam, kas iki 2007 metų rugsėjo 13 d. pirmasis paskelbs Ferma problemos sprendimą.

Nesigilindami į dramatišką Ferma problemos sprendimo istoriją, į jos sprendėjų (tarp jų ir patys žymiausi algebros, skaičių teorijos specialistai, ir mėgėjai – net ne matematikai, populiariai vadinami „fermatistais“) gautus rezultatus, paminėsime, kad Ferma problema, nors tiesiogiai ir nesusieta su kitomis svarbiomis matematikos problemomis, suvaidino labai didelį vaidmenį mokslo vystymosi istorijoje. Spręsdamas Ferma problemą, žymus vokiečių matematikas *E. Kumeris* (E. E. Kumer, 1810–1893) sukūrė *idealo* sąvoką, kuri prasiskverbė vos ne į visas matematikos šakas ir davė daug naujų rezultatų.

Na, o kokie šios problemos sprendimo rezultatai praėjus 80 metų nuo premijos paskelbimo ir iki termino pabaigos likus mažiau kaip 20 metų?

Anksčiau cituota P. Ferma pastaba Diofanto knygos paraštėje kitais žodžiais gali būti taip išreikšta: lygtis $x^n+y^n=z^n$ neišsprendžiama natūriniais skaičiais x, y ir z su bet kuriuo natūriniu rodikliu $n>2$.

Šio tvirtinimo (Ferma problemos) atskiri atvejai jau seniai išnagrinėti. Kad lygtis

$$x^4+y^4=z^4 \tag{11.10}$$

neišsprendžiama natūriniais skaičiais, įrodė dar pats Ferma. Jis sukūrė metodą, kurį galima pavadinti *nuoseklaus mažėjimo metodu.* Šiuo metodu Ferma labai didžiavosi, rašė, kad juo naudojosi visuose savo įrodymuose.

Šis Ferma metodas paremtas tokiu principu: *jeigu iš prielaidos, kad kuris nors natūrinis skaičius pasižymi tam tikra aibe savybių, išplaukia, jog egzistuoja mažesnis natūrinis skaičius, pasižymintis tomis pačiomis savybėmis, tai nė vienas natūrinis skaičius negali turėti minėtosios savybių aibės.*

Norėdami parodyti, kaip šiuo principu remiamasi įrodant, kad (11.10) lygtis neišsprendžiama natūriniais skaičiais x, y, z, trumpai aptarsime *Pitagoro trejetus.*

Pitagoro trejetu vadinami tokie trys natūriniai skaičiai x, y, z, su kuriais teisinga lygybė

$$x^2+y^2=z^2.$$

Pitagoro trejetas vadinamas primityviuoju, kai

$$\mathrm{D}(x, y, z)=1.$$

197 teorema. *Bet kurį primityvųjį Pitagoro trejetą galima išreikšti skaičiais*

$$2pq,\ p^2-q^2,\ p^2+q^2; \tag{11.11}$$

čia p ir q $(p>q)$ – skirtingo lyginumo tarpusavyje pirminiai skaičiai.

Įrodymas. Primityvųjį Pitagoro trejetą sudaro vienas lyginis ir du nelyginiai skaičiai. Tarkime, kad lyginis skaičius yra x. Tada $z+y$ ir $z-y$ yra lyginiai skaičiai. Pažymėkime juos taip: $z+y=2v$, $z-y=2w$. Iš lygybės $x^2=(z+y)(z-y)$ gauname $x^2=4uw$. Pažymėję $x=2u$, turime $u^2=vw$. Iš čia išplaukia (žr. 1 skyr., 100 užd.), kad v ir w yra kvadratai. Juos atitinkamai pažymėję p^2 ir q^2, matome, kad teoremos teiginys teisingas.

198 teorema. *Ferma lygtis*

$$x^4+y^4=z^4$$

neišsprendžiama natūriniais skaičiais.

Įrodymas. Tarkime, kad yra tokie natūriniai skaičiai x, y, z, su kuriais teisinga (11.10) lygybė. Galime tarti, kad D $(x, y, z)=1$. Tuomet skaičiai x^2, y^2, z^2 sudaro primityvųjį Pitagoro trejetą. Remiantis 197 teorema, egzistuoja tokie tarpusavyje pirminiai skirtingo lyginumo skaičiai p ir q, su kuriais teisingos lygybės

$$x^2=2pq,\ y^2=p^2-q^2,\ z^2=p^2+q^2.$$

Iš antrosios šių lygybių išplaukia, kad y, q, p sudaro primityvųjį Pitagoro trejetą. Tuomet p turi būti nelyginis, q – lyginis skaičius (jei q būtų nelyginis, p – lyginis skaičius, išeitų prieštaravimas, nes pasirinkus x lyginį, y ir z – nelyginius skaičius, lygybė $y^2+q^2=p^2$ būtų negalima – nelyginių skaičių kvadratų suma lygsta 2 moduliu 4, lyginio skaičiaus kvadratas lygsta 0 moduliu 4). Taigi egzistuoja skirtingo lyginumo tarpusavyje pirminiai skaičiai a ir b $(a>b>0)$, su kuriais teisingos lygybės

$$q=2ab,\ y=a^2-b^2,\ p=a^2+b^2.$$

Vadinasi,

$$x^2=2pq=4ab(a^2+b^2).$$

Ši lygybė reiškia, kad sandauga $ab(a^2+b^2)$ yra lyginio skaičiaus x pusės kvadratas. Skaičiai a ir b tarpusavyje pirminiai. Nesunku patikrinti, kad tada skaičiai ab ir a^2+b^2 taip pat tarpusavyje pirminiai. Kadangi jų sandauga – kvadratas, tai kiekvienas iš dauginamųjų irgi turi būti kvadratas. Pažymėkime $a=X^2$, $b=Y^2$ (jei tarpusavyje pirminių skaičių a ir b sandauga ab yra kvadratas, tai skaičiai a ir b taip pat kvadratai). Vadinasi, skaičius

$$X^4+Y^4=a^2+b^2$$

yra kvadratas; jį žymėkime Z^2.

Samprotaudami niekur nesirėmėme sąlyga, kad z^2 yra kvadratas. Rėmėmės prielaida, kad dviejų natūrinių skaičių x ir y ketvirtųjų laipsnių suma lygi kvadratui. Iš tos prielaidos išvedėme, kad mažesnių natūrinių skaičių X ir Y ketvirtųjų laipsnių suma taip pat lygi natūrinio skaičiaus kvadratui.

Remiantis anksčiau suformuluotu principu, jokių natūrinių skaičių 4-ųjų laipsnių suma negali būti lygi natūrinio skaičiaus kvadratui. Taigi ji negali būti lygi ir natūrinio skaičiaus ketvirtajam laipsniui. Teorema įrodyta.

Ferma lygtis, kai $n=3$, pasirodė esanti sudėtingesnė už ką tik nagrinėtąją. 1770 metais jos neišsprendžiamumą įrodė Oileris, naudodamasis kompleksiniais skaičiais ($a+b\sqrt{-3}$ pavidalo).

1825 m. Ležandrui pavyko įrodyti, kad lygtis $x^5+y^5=z^5$ neišsprendžiama natūriniais skaičiais. 1839 m. G. Lamė įrodė, kad neišsprendžiama ir Ferma lygtis, kai $n=7$.

Tačiau patys svarbiausi rezultatai buvo gauti jau minėto Kumerio. Ferma problemai spręsti jis sukūrė algebrinius metodus, kurių vertė nesumenkė-

jusi iki šiol. Kumeris įrodė, kad Ferma hipotezė teisinga plačiai pirminių rodiklių $n=p$ klasei (vadinamiesiems *reguliariems* pirminiams skaičiams).

Kumerio sukurti metodai buvo toliau vystomi ir tobulinami. Jau šiame amžiuje atskiriems Ferma problemos atvejams tirti buvo pasitelktos elektroninės skaičiavimo mašinos. Pavyzdžiui, 1976 m. Ferma hipotezė buvo patikrinta tais atvejais, kai rodiklis n yra intervale $3 \leqslant n < 125\,000$ ir kai n yra pirminis skaičius p,

$$p < 714\ 591\ 416\ 091\ 389.$$

Atsižvelgiant į tai, kad skaičius 2^{125000} užrašomas 37628 skaitmenimis, pastangos rasti Ferma hipotezei prieštaraujantį pavyzdį atrodo beviltiškos.

Ferma lygtį galima užrašyti

$$x^n + y^n = 1 \tag{11.12}$$

pavidalu ir ieškoti pastarosios lygties racionaliųjų sprendinių.

(11.12) lygtis Euklido plokštumoje reiškia kreivę F_n, kuri vadinama n-osios *eilės Ferma kreive*. Ferma hipotezės tvirtinimas reiškia, kad, kai $n > 2$, vieninteliai Ferma kreivės racionalieji taškai yra jos susikirtimo su koordinačių ašimis taškai. Pastaraisiais metais, tiriant kreivių racionaliuosius taškus, gauta daug svarbių rezultatų, taigi žengtas dar vienas svarbus žingsnis sprendžiant Ferma problemą.

Nežiūrint šių rezultatų, Ferma problemos sprendėjai nepraranda vilties surasti labai paprastą, elementarų sprendimą. Tokių sprendėjų pasaulyje gana daug, jų yra ir Lietuvoje. Todėl matematikos mokytojui reikėtų žinoti ir šio klausimo specialistų vieningą nuomonę – beveik neįtikėtina, kad galėtų būti koks nors elementarus problemos sprendimas.

Ferma lygtis pasižymi paprastumu, tam tikra simetrija. Galima parašyti daug kitokių Diofanto lygčių, nepasižyminčių panašia simetrija. Ar jos išsprendžiamos, kaip rasti sprendinius? Bendro atsakymo nėra, reikia nagrinėti kiekvieną konkrečią lygtį.

Išnagrinėkime lygties

$$x^2 + x = 2y^2 \tag{11.13}$$

sprendimą.

Nesunku įsitikinti: jeigu sveikųjų skaičių x, y pora yra tos lygties sprendinys, tai sprendinys yra ir skaičių pora

$$u = 3x + 4y + 1, \quad v = 2x + 3y + 1. \tag{11.14}$$

Tarkime, kad x, y $(x > 1)$ yra (11.13) lygties sprendinys. Tada ir $y > 1$. Įrodysim, kad tuo atveju teisingos nelygybės

$$3x - 4y + 1 > 0, \ 3y - 2x - 1 > 0, \ 2x - 4y + 1 < 0. \tag{11.15}$$

Iš tikrųjų, jei būtų $4y \geqslant 3x + 1$, tai turėtume

$$16y^2 \geqslant 9x^2 + 6x + 1,$$

ir iš (11.13) išplauktų

$$2x \geqslant x^2 + 1.$$

Tai prieštarautų prielaidai, kad $x > 1$.

Panašiai įrodoma ir antroji iš trijų (11.15) nelygybių. Trečioji nelygybė yra pirmųjų dviejų išvada.

Pažymėsime

$$\xi = 3x - 4y - 1, \quad \eta = 3y - 2x - 1. \tag{11.16}$$

Iš (11.15) nelygybių išplaukia, kad ξ ir η yra natūriniai skaičiai, $\xi < x$, jie sudaro (11.13) lygties sprendinį. Toliau šiame paragrafe skaičių a ir b didžiausią bendrąjį daliklį žymėsime $D(a, b)$.

Apibrėšime skaičių poros (x, y) transformacijas f ir g formulėmis

$$f(x, y) = (3x + 4y + 1, \ 2x + 3y + 1),$$

$$g(x, y) = (3y - 4y + 1, \ 3y - 2x - 1).$$

Transformacijas galima atlikti pakartotinai. Pažymėkime

$$f_{k+1} = f\big(f_k(x, y)\big),$$

$$g_{k+1} = g\big(g_k(x, y)\big), \quad k \geqslant 1.$$

Lengva įrodyti lygybę

$$f\big(g(x, y)\big) = (x, y).$$

Remiantis indukcija, su bet kuriuo natūriniu n

$$f_n\big(g_n(x, y)\big) = (x, y).$$

Kaip minėjome, jeigu (x, y) yra tokia (11.13) lygties sprendinį sudarančių natūrinių skaičių pora, kurioje $x > 1$, tai

$$(\xi, \eta) = g(x, y)$$

yra kita tos lygties sprendinį sudarančių skaičių pora, ir $\xi < x$. Jeigu $\xi > 1$, tai $(\xi_1, \eta_1) - g(\xi, \eta) = g_2(x, y)$ yra taip pat (11.13) lygties sprendinys; čia $\xi_1 < \xi$. Kadangi mažėjanti natūrinių skaičių x, ξ_i seka yra baigtinė, tai po n žingsnių gausime (11.13) lygties sprendinį u, v, su kuriuo teisingos lygybės

$$(u, v) = g_n(x, y) \quad \text{ir} \quad u = 1.$$

Tačiau, jei pora u, v yra (11.13) sprendinys ir $u = 1$, tai ir $v = 1$. Vadinasi, yra toks natūrinis skaičius n, su kuriuo

$$g_n(x, y) = (1, 1). \tag{11.17}$$

Taigi iš lygybės $f_n g_n(x, y) = (x, y)$ išplaukia

$$(x, y) = f_n(1, 1). \tag{11.18}$$

Skaičių pora (1, 1) yra (11.13) lygties sprendinys — tai akivaizdu. Bet kuris kitas sprendinys (x, y) išreiškiamas (11.18) formule. Gautąjį rezultatą apibendrinsime šitokia teorema.

199 teorema. *Lygties*

$$x^2 + x - 2y^2 = 0$$

sveikieji sprendiniai apibrėžiami rekurentinėmis formulėmis

$$x_{n+1} = 3x_n + 4y_n + 1,$$
$$y_{n+1} = 2x_n + 3y_n + 1,$$
$$x_1 = 1, \quad y_1 = 1.$$

Šios teoremos įrodymo būdas gali būti pritaikytas ir kai kurioms kitoms Diofanto lygtims spręsti. Panašiai galima nagrinėti lygtį

$$x^2 + x + 1 = 3y^2$$

ir kai kurias kitas.

Trumpai aptarsime dar vieną Diofanto lygtį.

200 teorema. *Visi natūriniai lygties*

$$xy = zt \tag{11.19}$$

sprendiniai apibrėžiami formulėmis

$$x = ac, \quad y = bd, \quad z = ad, \quad t = bc;$$

čia a, b, c, d *– bet kokie natūriniai skaičiai,* $\mathrm{D}(c, d) = 1$.

Įrodymas. Tarkime, kad natūriniai skaičiai x, y, z, t yra (11.19) lygties sprendinys. Pažymėkime raide a skaičių x ir z didžiausią bendrąjį daliklį. Tada egzistuoja tarpusavyje pirminiai natūriniai skaičiai c ir d, su kuriais

$$x = ac, \quad z = ad.$$

Iš (11.19) lygybės išplaukia $cy = dt$. Kadangi $\mathrm{D}(c, d) = 1$, tai yra toks natūrinis skaičius b, su kuriuo teisinga lygybė

$$y = bd.$$

Iš čia išplaukia

$$t = bc.$$

Įrodėme, kad visi (11.19) lygties natūriniai sprendiniai yra tarp skaičių, kurie rašomi formulėmis, turinčiomis 4 laisvuosius parametrus a, b, c, d. Tačiau visus tuos sprendinius galima gauti ir naudojantis tik trimis parametrais iš formulių

$$y = \frac{uz}{d}, \quad t = \frac{ux}{d};$$

čia x, z, u – bet kokie natūriniai skaičiai, d – skaičių x ir y didžiausias bendrasis daliklis.

Indeksų ir antiindeksų lentelės

Pirminis skaičius 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

i	0	1	2	3	4	5	6	7	8	9
0	1	2								

Pirminis skaičius 5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Pirminis skaičius 7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

i	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Pirminis skaičius 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Pirminis skaičius 13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Pirminis skaičius 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Pirminis skaičius 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Pirminis skaičius 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

i	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Pirminis skaičius 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Pirminis skaičius 31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Pirminis skaičius 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Pirminis skaičius 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

i	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Pirminis skaičius 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Pirminis skaičius 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

i	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	12	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Pirminis skaičius 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Pirminis skaičius 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	18	37	15	30		

Pirminis skaičius 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	46	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Pirminis skaičius 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Pirminis skaičius 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

i	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Pirminis skaičius 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

i	0	1	2	3	4	5	6	7	8	9
0	1	5	25	5	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	8	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Pirminis skaičius 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	45	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Pirminis skaičius 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Pirminis skaičius 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

i	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

Pirminių skaičių, ne didesnių kaip 1000, lentelė

2	47	109	191	269	353	439	523	617	709	811	907
3	53	113	193	271	359	443	541	619	719	821	911
5	59	127	197	277	367	449	547	631	727	823	919
7	61	131	199	281	373	457	557	641	733	827	929
11	67	137	211	233	379	461	563	643	739	829	937
13	71	139	223	293	383	463	569	647	743	839	941
17	73	149	227	307	389	467	571	653	751	853	947
19	79	151	229	311	397	479	577	659	757	857	953
23	83	157	233	313	401	487	587	661	761	859	967
29	89	163	239	317	409	491	593	673	769	863	971
31	97	167	241	331	419	499	599	677	773	877	977
37	101	173	251	337	421	503	601	683	787	881	983
41	103	179	257	347	431	509	607	691	797	883	991
43	107	181	263	349	433	521	613	701	809	887	997

Uždavinių atsakymai ir nurodymai

I skyrius

3. $x=1/2$. **5.** 2. **6.** Nurodymas. Tarkite priešingai – yra 2 skirtingi skaičiaus b papildomieji dalikliai. **8.** $a=b$. **10.** Nurodymas. Iš trupmenos $(mq+pn)/(m-p)$ atimkite trupmeną $(mn+pq)/(m-p)$. **11.** Nurodymas. Įrodykite, kad trijų iš eilės einančių natūrinių skaičių sandauga dalijasi iš 6. Pakeiskite $2n+1=n-1+(n+2)$. **14.** Antrasis skaičius $121+121!$, bet trečiasis skaičius jų neturi. **15.** a) 11; b) 3; c) 1. **16.** b) 0; d) 1. **17.** a) -1; b) -32; c) 2. **18.** a) -1; b) -1; c) 1. **19.** 151. **20.** a) neišsprendžiama; b) neišsprendžiama; c) [2, 3) ir $[-3, -2)$; d) $x=7/2$. **21.** 69. **25.** $r_3=-(q_1+q_3+q_1q_2q_3)a+(1+qq_1+$

$+qq_3+q_2q_3+qq_1q_2q_3)b$. **26.** $r=720-(-47)(-15)$, $r_1=720\cdot 4+(-47)6$, $r_2=720(-3)-(-47)46$, $r_3=720\cdot 22+(-47)337$. **28.** $101_2=7_8$, $1011011=133_8$. **30.** $11_2=3$, $110_2=6$, $10111_2=23$. **31.** 5120_6, 78_9, 461524_7, 4. **32.** $4010=30322_6$, $312_4=130_6$, $157_8=303_6$. **33.** $421=265_{13}$, $181_9=aa_{13}$ (a – vienaženklis skaitmuo 13-ainėje sistemoje, lygus 11). **34.** $315_8-315_7=46=56_8=64_7$. **35.** $g=5$ arba $g=7$. **36.** 150, 145, 295, $g=15$. **37.** 503_7. **41.** Nesudaro. **44.** 24 $(4t+1)-96t$. **47.** Pirmoji lygtis neturi. **48.** Nurodymas. Skaičių ak ir bk natūrinių kartotinių aibė (bendrųjų kartotinių) sutampa su skaičiaus k $[a, b]$ natūrinių kartotinių aibe. **49.** Nurodymas. Sudėję šias trupmenas, įrodykite, kad $(2a+b, a+b)=1$. **57.** Nurodymas. Raskite tokius x ir y, su kuriais $(2n+1)x-(9n+4)y=1$. **58.** Nurodymas. Nagrinėkite, kai n – lyginis (jei n – nelyginis, vienu iš tų skaičių galima imti 2). **60.** Nurodymas. Naudokitės kubų skirtumo formule. **64.** Tik 5927, 5939. **69.** $n=1$. **70.** $a=3$. **77.** Nurodymas. Visi sudėtiniai skaičiai, mažesni už 30, nėra su 30 tarpusavyje pirminiai. **81.** Nurodymas. Jei $d \mid p$, tai $2^d-1 \mid 2^p-1$. **82.** Nurodymas. Naudokitės skirtumu $(m+n)^2-(m^2+n^2)$. **83.** Nurodymas. Iš pradžių įrodykite štai ką: jei skaičius N yra $N=2^a3^b$ pavidalo, tai jis turi $(a+1)(b+1)$ natūrinių daliklių. **84.** Nurodymas. Taikykite matematinę indukciją. **85.** Nurodymas. Naudokitės 86 uždaviniu. **86.** Nurodymas. Įrodykite, kad binomo $(a+b)^p$ visi koeficientai, išskyrus kraštinius, dalijasi iš p. **87.** Nurodymas. Skaičius n negali būti nei $3k$, nei $3k-1$ formos. *Ats.* $n=6m+1$. **94.** 253125. **95.** 28. **96.** 120. **97.** 192. **106.** $\tau(150)=12$, $\tau(250)=8$. **107.** $\tau(45)=156$, $\tau(124)=224$. **108.** Nurodymas. Visuomet arba skaičiaus n daliklis, arba jo papildomasis daliklis yra $\geqslant\sqrt{n}$. **109.** Nurodymas. Įrodykite, kad skaičiaus n daliklių kubų suma $\sigma_3(n)$ yra multiplikacinė funkcija. **110.** 82. **111.** 12. **112.** $a=7t+2$, $7t+3$, $7t+5$ ($t\in\mathbf{Z}$). **113.** Nurodymas. Nustatykite, kaip kinta skaičių x^2 ir 2^x dalybos iš 7 liekanos, kintant x. *Ats.* 7142. **114.** Nurodymas. Pakanka ištirti už 7 mažesnių natūrinių skaičių dalybos iš 7 liekanas. *Ats.* 0, 1, 6. **116.** Nurodymas. Taikykite matematinę indukciją. **118.** $213820<\pi(10!)<266675$. **119.** c) $2^{65}<p_n<2^{68}$.

II skyrius

1. $125/31=[4, 31]$, $49/45=[1, 11, 4]$. **2.** $2086/6854=7/23$. **3.** $[1, 2, 3, 4, 5]=225/157$. **4.** $[a, b, c, d]=(1+ab+ad+cd+abcd)/(b+d+bcd)$. **5.** Pirmosios lygties $x=3$. **6.** -3, $1=[-4, 1, 9]$, $(-3/7)^{-2}=[5, 2, 4]$. **9.** Skaičiui $[1, 2, 3, 4]$ $r_0=43/30$, $r_1=30/13$, $r_2=13/4$, $r_3=4$. **10.** a) $\alpha-R_4=0$, $|\alpha-R_3|<1/52$, $|\alpha-R_2|<1/6$, $|\alpha-R_1|<1/2$, $|\alpha-R_0|<1$. **12.** 5/2. **13.** 1/2, 1/3, 1/5, 1/7, 2/5, 3/7, 2/7. **16.** 3. **17.** $2\sqrt{3}=[3, \overline{2, 6}]$. **18.** Skaičiaus $\sqrt{3}$ grandininės trupmenos elementai q_n ir skaičiaus $-\sqrt{3}$ grandininės trupmenos elementai p_n susieti lygybe $q_n=p_{n+2}$. **19.** Skaičiaus π tokios trupmenos yra 333/106 ir 355/113, kitų skaičių jos sutampa su tais skaičiais. **20.** 545/106, 581/113. **21.** 1/1424. **22.** $|e-R_4|>1/273$. **23.** $2\sqrt{5}\sim 313/70$. **26.** a) be reduktų, geriausi artiniai dar yra trupmenos $-4/3$, $-7/5$, $-10/7$. **29.** $\sqrt{7}=[2, \overline{1, 1, 1, 4}]$, $2\sqrt{7}=[5, \overline{3, 2, 3, 10}]$. **30.** Lygties $x^3+x+1=0$ šaknis $x=[-1, 3, 6, 1, 3, \ldots]$. **31.** $[\overline{1, 4}]=(1+\sqrt{2})/2$, $[1, \overline{4, 5, 1}]=9(34-9\sqrt{5})/236$. **32.** Jei $b>1$ – skleidinys $[a-c-1, 1, b-1, c, b]$, jei $b=1$, tai $[a-c-1, c+1, \overline{1, c}]$. **34.** R_6 išreiškia $-\sqrt{7}$ tikslumu 10^{-3}. **35.** 63/44. **36.** Pirmosios lygties sprendiniai $x=-14+13t$, $y=14-12t$ ($t\in\mathbf{Z}$). **37.** (1, 21), (1, 1), (22, 46). **38.** 1) $d=3a-b$. **39.** $a=d+3t$, $b=d+2t$ ($t\in\mathbf{Z}$). **40.** $u_n=Q_{n-1}=P_{n-2}$ ($n>1$).

III skyrius

2. 1) $t=4+11n$ ($n\in\mathbf{Z}$). **3.** 1) $m=2, 3, 5, 6, 9, 10, 15, 30, 45, 90$. **4.** 4) $3\equiv 10 \pmod 7$. **7.** 1) $-14\in K_0$, $11\in K_4$, $-13\in K_1$. **10.** $a=3+7t$ ($t\in\mathbf{Z}$). **12.** 1) $K_3+K_{97}=K_9$. **14.** Jeigu $a=5$, $x=8$. **24.** Pilnųjų liekanų sistemų 3^6. **26.** Moduliu 8: $(K_7)^{-1}=K_7$, $(K_5)^{-1}=K_3$. **28.** $x=2^k$. **29.** Pirmosios lygties sprendiniai $x=2^kp_1p_2\ldots p_r$; čia p_j-2t+1 pavidalo pirminiai skaičiai. **30.** Pirmasis. **32.** 30. **34.** $\varphi(24)=8$. **35.** 2. **36.** m. **37.** Pirmojo skaičiaus liekana 16. **42.** 1) sekmadienis.

IV skyrius

3. 1) su visomis turi; 2) 6. **5.** 2) $x\equiv 6 \pmod{11}$. **7.** 1) $x\equiv 7 \pmod{22}$, $x\equiv 18 \pmod{22}$. **8.** Nurodymas. Lygtį pakeiskite lyginiu moduliu 5, paskui lyginiu moduliu 3. 1) *Ats.* $x=7, 2, 4, -1$; 2) *Ats.* $(-6, -61)$, $(-1, -1)$, $(1, 1)$, $(6, 41)$. **9.** $x_1=152$, $x_2=656$.

10. Nurodymas. Iš būtinosios sąlygos gaukite $x=1+2t$ ($t\in\mathbf{Z}$). **11.** 1) $x\equiv 939 \pmod{2145}$; 2) $x\equiv 446 \pmod{693}$. **12.** 2) $x\equiv 80 \pmod{81}$. **13.** 1) $x\equiv 1 \pmod 5$; 2) $x\equiv 2 \pmod 3$. **14.** 1) $y^2\equiv 5 \pmod{13}$. **15.** 2) K_1, K_3, K_4, K_5, K_9. **18.** 43, 44, 46. **19.** 1) išsprendžiamas. **20.** 31, 33, 34. **22.** 1) neišsprendžiamas. **24.** 1) neišsprendžiamas. **29.** Nurodymas. Naudokitės lyginiu moduliu 4. **30.** Nurodymas. Lyginį pakeiskite lyginių sistema moduliais 4 ir p. **31.** Nurodymas. Sumą pakeiskite lyginiu moduliu 10. **32.** $p=12k\pm 1$.

V skyrius

1. $r_{13}(10)=6$, $r_{13}(11)=12$, $r_{13}(12)=2$. **2.** Moduliu 16: 1, 2, 4, 8, moduliu 17: 1, 2, 4, 8, 16. **3.** 4, 6, 5, 9, 16, 17. **4.** Moduliu 14: 3, 5. **5.** Moduliu 49: $a\equiv 3 \pmod 7$, $a\equiv 5 \pmod 7$. **6.** Moduliu 18: 5, 7. **7.** 1) 16; 2) 24; 3) 24. **8.** 1) 2; 2) 5; 3) 3. **12.** $x\equiv 9 \pmod{47}$. **13.** $x\equiv 16 \pmod{19}$. **14.** $x\equiv 69 \pmod{73}$. **16.** 1, 11, 18, 1, 13. **18.** 2, 1, 2, 1, 3.

VI skyrius

1. 1–3) $\mathbf{Z}[\sqrt{2}]\subset\mathbf{R}$, $\mathbf{Z}[\sqrt[3]{2}]\subset\mathbf{R}$, $\mathbf{Z}[i]\subset\mathbf{K}$, $\mathbf{R}$ ir $\mathbf{K}$ – laukai. Todėl užtenka patikrinti, ar teisingos 90 teoremos sąlygos. **2.** Komutatyvusis žiedas. $O=(0, 0)$, $e=(1, 1)$. Vieneto dalikliai – (l, t), $l, t\in\{-1, 1\}$. Ekvivalentumo klasės – $K_{(m,n)}=\{(m, n), (-m, n), (m, -n), (-m, -n)\}$. **3.** Vieneto dalikliai – $l+k\sqrt{m}$, (l, k) – lygčių $x^2-2y^2=\pm 1$ sprendiniai. **4, 5, 6.** Naudokitės 90 teorema. **7.** Vieneto dalikliai – klasės K_r, $D(r, 24)=1$. Klasei K_l asocijuotų elementų (klasių) aibė – $\{K_lK_r \mid D(r, 24)=1\}$. **8.** Ne. Nors komutatyvus, bet turi nulio daliklių. **10.** Išspręskite lygtį $(m, n)(xy)=(0, 0)$. **18.** Nagrinėkite funkciją $f(8t+r)=K_r$, $r=0, 1, \ldots 7$. Išstudijuokite sąvokas. **19.** Studijuokite sąvokas. **24.** Apibrėžkite $g(m+n\sqrt{2})=|m^2-2n^2|$ ir išnagrinėkite 57 paragrafo 2 pavyzdį. **25.** 1) kadangi $\alpha=\beta(4-i)-1$, tai $D(\alpha, \beta)=1$; 2–3) $D(\alpha, \beta)=1$, $M(\alpha, \beta)=\alpha\beta$. **26.** 1) $D(\alpha, \beta)=\beta$, $M(\alpha, \beta)=\alpha$; 2) $\alpha=\beta(1+\sqrt{2})-\sqrt{2}$, $\beta=3\sqrt{2}+1$, todėl $D(\alpha, \beta)=1$, $M(\alpha, \beta)=\alpha\beta$; 3) $D(\alpha, \beta)=\sqrt{2}$, $M(\alpha, \beta)=14\cdot 7\sqrt{2}$. **28.** 1) $\mathbf{Q}[i]$; 2) $\mathbf{Q}[\sqrt{2}]$; 3) $\mathbf{Q}[\sqrt{3}]$.

VII skyrius

3. Nagrinėkite $\check{\mathbf{Z}}[x^n]$, $n=1, 2, 3, \ldots$ **4.** Sveikųjų skaičių žiede $e=1$, $O=0$. **5.** a) 1; -12; $11\sqrt{2}-11$; b) $-2\sqrt{3}$, $-\sqrt{3}+5$; $34\sqrt{3}$; c) $-7-5i$; $-11i$; $-10-9i$. **6.** $f(O)=a_0$, $f(e)=\sum_{j=0}^{n} a_j$, $f(-e)=\sum_{j=0}^{n}(-1)^j a_j$. **7.** 1) a) nelygios; b) nelygios; c) lygios; 2) a) nelygios; b) lygios; c) lygios. **10.** a) $-\frac{7}{2}x^2+\frac{5}{2}x+3$; b) $6x^2+11x-35$; c) x^3+2x^2-3x-5; d) $x^4-2x^3+3x^2+2$. **12.** a) ir b) Pastebėkite, kad $\sum_{j=0}^{n} a_j(x^k)^j=\sum_{j=0}^{nk} c_j x^j\in\check{\mathbf{Z}}[x]$. Įrodykite, kad funkcija $\varphi\left(\sum_{j=0}^{n} a_j(x^k)^j\right)=\sum_{j=0}^{n} a_j x^j$ yra žiedų $\check{\mathbf{Z}}[x^k]$ ir $\check{\mathbf{Z}}[x]$ izomorfizmas; c) kadangi $\mathbf{R}_n[x]\subset\mathbf{R}[x]$, o $\mathbf{R}[x]$ yra vektorinė erdvė, tai užtenka remtis teorema apie poerdvius (žr. 1 d., 90 teoremą). Paprasčiausia bazė yra $1, x, x^2, \ldots, x^n$. **17–18.** Naudokitės Hornerio schema. **21.** Remkitės 139 teorema ir dalumo savybėmis. **22.** a) ir b) raskite polinomo $g(x)$ šaknis ir patikrinkite, ar jos yra polinomo $f(x)$ šaknys. **23.** a–c) algebriniai antrojo laipsnio; d–e) algebrinis ketvirtojo laipsnio; f) algebrinis šeštojo laipsnio. **24.** Remkitės tuo, kad polinomų $f(x)$ ir $cf(x)$ šaknys sutampa. **25.** Sudarykite polinomą su realiaisiais koeficientais, kurio šaknis yra $a+ib$.

2. a) dalijasi; b) nesidalija; c) nesidalija. **3.** a) 1; b) $-1, 0$; c) $0, -1$. **4.** a) kadangi $f(x)=(x-1)(3x+9)+8$, tai $f(x)\in K_8=\{(x-1)h(x)+8 \mid h(x)\in \mathbf{Z}[x]\}$. $\varphi(x)=(x-1)\times$ $\times(3x^2-3x+1)+5$, tai $\varphi(x)\in K_5=\{(x-1)h(x)+5 \mid h(x)\in \mathbf{Z}[x]\}$. $K_8+K_5=K_{13}=\{(x-1)\times$ $\times h(x)+13 \mid h(x)\in \mathbf{Z}[x]\}$, K_8, $K_5=K_{40}=\{(x-1)h(x)+40 \mid h(x)\in \mathbf{Z}[x]\}$; b–e) sprendžiami analogiškai. **5.** a) x^2-2x+1; b) $2x^2-1$; c) x^5+3x^4+2x-6; d) 1; e) $\sqrt{2}x^3+\pi x-4$; f) $(2-i)x^4-ix^2+(1-i)$. **6.** a) $D(x)=x^2-2x+1$, $u(x)=-\frac{1}{123}(x-11)$, $v(x)=$ $=\frac{1}{123}(3x^3-33x^2-6x+67)$; b) $D(x)=x^2+2$, $u(x)=\frac{27}{110}$, $v(x)=\frac{1}{110}(-63x^2+$ $+21x+29)$; c) $D(x)=1$, $u(x)=2x^2+3$, $v(x)=-1$; d) $D(x)=x$, $u(x)=1$, $v(x)=2x^2-$ -1. **7.** a) x^2+4; b) 1. **8.** a) $\frac{1}{438}(-65\alpha^2-25\alpha+69)$; b) $\frac{1}{12}(3\alpha^2-17\alpha+31)$. **9.** a) $\frac{1}{10}(\sqrt[3]{4}-2\sqrt[3]{2}+4$; b) $\frac{3}{253}(67\sqrt[3]{4}+77\sqrt[3]{2}+106)$; c) $\frac{1}{769}(16\sqrt[4]{27}+77\sqrt[4]{9}-$ $-62\sqrt[4]{3}-10)$; d) $(\sqrt[3]{3}-2)(2\sqrt[3]{9}+3\sqrt[3]{3}+4)$. e) $-\frac{1}{229}(\sqrt[3]{3}+2\sqrt[3]{2})(12\sqrt[3]{4}+$ $+32\sqrt[3]{2}+4)$, **13.** a) neturi; b) turi; c) turi; d) neturi. **14.** a) $(x^2+2)^2(x-3)$; b) $(x+1)^3\times$ $\times(x+2)^2(x-3)$; c) $(x+2)^3(2x^2-3)^2$; d) $(2x+1)^4(3x-1)$; e) $(x+\sqrt{2})^3x^2(x-\sqrt{2})$. **15.** Remkitės šaknies kartotinumo apibrėžimu ir 155 teorema. **16.** Naudokitės 15 uždaviniu ir, sudarę tiesinių lygčių sistemą, raskite p, q, r.

IX skyrius

10. a) $\sigma_1^2-2\sigma_2(1+\sigma_1)$; b) $\sigma_1^3+\sigma_1^2-5\sigma_2-3\sigma_1\sigma_2$; c) $\sigma_1^2\sigma_2-9\sigma_1^2+5\sigma_2^2+16\sigma_2$; d) $\sigma_1^2-2\sigma_2$. e) $3\sigma_3^2-\sigma_1\sigma_3$; f) $\sigma_1^2-2\sigma_2$; g) $\sigma_1^3-3\sigma_1\sigma_2+2\sigma_3$; h) $1+2\sigma_1+4\sigma_2+8\sigma_3$; i) $\sigma_1\sigma_2-\sigma_3$; **11.** Naudokitės Vieto formulėmis. **12.** a–c) Simetrinį polinomą išreikškite pagrindiniais simetriniais polinomais, po to naudokitės Vieto formulėmis. **13.** a) $-\frac{1}{6}(7\sqrt[3]{4}+$ $+8\sqrt[3]{2}+10)$; b) $\frac{1}{6}(\sqrt[3]{5}+1)$; c) $\frac{1}{14}(8-4\sqrt[4]{2}+2\sqrt[4]{4}-\sqrt[4]{8})$; d) $\frac{1}{2}(\sqrt[5]{81}+\sqrt[5]{27}+$ $+\sqrt[5]{9}+1)$.

X skyrius

1. a) $(x-3)(x^2+3x+9)=(x-3)(x+3)\left(\frac{1}{2}-\frac{i\sqrt{3}}{2}\right)(x+3)\left(\frac{1}{2}+\frac{i\sqrt{3}}{2}\right)$; b) $(x-2)(x-3)$; c) $(x^3-4)(x^3+4)=(x-\sqrt[3]{4})(x^2+\sqrt[3]{4}x+\sqrt[3]{16})(x^3+4)=\prod_{j=0}^{5}(x-\varepsilon_j\sqrt[3]{4})$; čia ε_j ($j=0, 1, 2, 3, 4, 5$) – vieneto 6-ojo laipsnio šaknys; d) $(x^2-2x+2)(x^2+2x+$ $+2)=\big(x-(1+i)\big)\big(x-(1-i)\big)\big(x+(1-i)\big)\big(x+(1+i)\big)$; e) $(x-\sqrt{5+2\sqrt{6}})(x+\sqrt{5+2\sqrt{6}})\times$ $\times(x-\sqrt{5-2\sqrt{6}})(x+\sqrt{5-2\sqrt{6}})$; f) $(x-1)^2(x+1)^2(x^2+1)^2=(x-1)^2(x+1)^2(x-i)^2\times$ $\times(x+i)^2$. **2.** a–c) Naudokitės skaidiniu $f(x)=\prod_{j=1}^{m}(x-l_j)^{s_j}$. Sudauginę gausite polinomą. **3.** Remkitės 3 lema ir 2 uždavinio nurodymu. **4.** a) $-1, 1, -2, 2$; b) $2, 4, 5$;

c) $-6, \frac{1}{2}$; d) $\frac{1}{2}, \frac{1}{3}$; e) $-\frac{3}{7}, 1, -3, 3$; f) $\frac{1}{3}, \frac{3}{2}, \frac{7}{4}$. **5.** a) $-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}$, $-1, 1$; *b*) $-\sqrt{2}, \sqrt{2}, -\sqrt{5}, \sqrt{5}$; c) $-1, 1, -i, i, -\sqrt{2}, \sqrt{2}, -i\sqrt{2}$, $i\sqrt{2}$; d) $-\sqrt[3]{6}, \sqrt[3]{6}\left(\frac{1}{2}+\frac{i\sqrt{3}}{2}\right), \sqrt[3]{6}\left(\frac{1}{2}-\frac{i\sqrt{3}}{2}\right), \frac{1}{\sqrt[3]{2}}, \frac{1}{\sqrt[3]{2}}\left(-\frac{1}{2}+\right.$ $\left.+\frac{i\sqrt{3}}{2}\right), \frac{1}{\sqrt[3]{2}}\left(-\frac{1}{2}-\frac{i\sqrt{3}}{2}\right)$; e) $-1, 1, -i, i, \frac{1}{2}\sqrt[4]{\frac{12}{7}}(1+i)$, $\frac{1}{2}\sqrt[4]{\frac{12}{7}}(1-i), \frac{1}{2}\sqrt[4]{\frac{12}{7}}(-1+i), -\frac{1}{2}\sqrt[4]{\frac{12}{7}}(1+i)$; f) $\sqrt{2}, -\sqrt{2}, -2$, $2, -\sqrt{5}, 5$; g) $\frac{3-\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}, -\frac{1}{2}+i\frac{\sqrt{3}}{2}, -\frac{1}{2}-i\frac{\sqrt{3}}{2}$; h) $l_1=$ $=-1$, $l_2=l_3=l_4=\frac{1}{2}+i\frac{\sqrt{3}}{2}$, $l_5=l_6=l_7=\frac{1}{2}-i\frac{\sqrt{3}}{2}$. **6.** a–c) pirmiausia raskite racionaliąsias, po to iracionaliąsias šaknis ir tada užrašykite skaidinius. a) $(x+1)(2x-1)\times$ $\times(3x+2)(x^2-3x-3)(x^2-3x+3)=(x+1)(2x-1)(3x+2)\left(x-\frac{1}{2}(3+\sqrt{21})\right)\left(x-\frac{1}{2}(3-\right.$ $\left.-\sqrt{21})\right)(x^2-3x+3)=(x+1)(2x-1)(3x+2)\left(x-\frac{1}{2}(3+\sqrt{21})\right)\left(x-\frac{1}{2}(3-\sqrt{21})\right)\times$ $\times\left(x-\frac{1}{2}(3+i\sqrt{3})\right)\left(x-\frac{1}{2}(3-i\sqrt{3})\right)$; b) $1, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, -2, \frac{1}{2}(1+i\sqrt{3})$. $\frac{1}{2}(1-i\sqrt{3})$. **9.** a) $f(x)$, x^2-2x+3, $4x-9$, -1; $l\in[0, 1]$; b) $f(x)$, $f'(x)$, $3x+1$, 1; $l_1\in[0, 1]$, $l_2\in[2, 3]$; c) $f(x)$, $f'(x)$, $-5x^2+22$, $-8x-13$, -1; $l_1\in[-2, -1]$, $l_2\in[0, 1]$.

Literatūra

1. **Matuliauskas A.** Algebra. V.: Mokslas, 1985.
2. **Бухштаб А. А.** Теория чисел. М.: Просвещение, 1966.
3. **Ван дер Варден Б. Л.** Алгебра. М.: Наука, 1976.
4. **Виноградов И. М.** Основы теории чисел. М.: Наука, 1981.
5. **Грибанов В. Ч., Титов П. И.** Сборник упражнений по теории чисел. М.: Просвещение, 1964.
6. **Куликов Л. Я.** Алгебра и теория чисел. М.: Высшая школа, 1979.
7. **Курош А. Г.** Курс высшей алгебры. М.: Наука, 1975.
8. **Окунев Л. Я.** Высшая алгебра. М.: Просвещение, 1966.

Dalykinė rodyklė

Abelis 384
Algebrinis elementas 259
– lauko uždarumas 260
– skaičius 259, 373
Algebriniai jungtiniai elementai 260
Algebrinio elemento laipsnis 260
– – minimalusis polinomas 365
Algoritmas Euklido 12
– – polinomų žiede 267
– – žiede 216
– polinomo racionaliosioms šaknims rasti 336
Bezu 252
Dalikliai nulio 111
– vieneto 195
Daliklis elemento 199
– polinomo 247
– skaičiaus 6
– bendrasis elementų 212
– – – didžiausias 212
– – polinomų 265
– – – didžiausias 266
– – skaičių 23
– – – didžiausias 23
– pirminis elemento 217
– – polinomo 277
– – skaičiaus 43
– tiesioginis elemento 201
– – polinomo 248
– – skaičiaus 8
– trivialusis elemento 201
– – polinomo 248
– – skaičiaus 8
Daklilių tiesioginių seka 248
Dalumo sąryšis integralumo srityje 198
– – polinomų žiede 247
– – sveikųjų skaičių žiede 6
Daugikliai kartotiniai polinomo 289
Daugiklio kartotinumas 289
Didžiausiojo skaičiaus principas 5
Diofantas 36
Diskriminantas polinomo 323
Eizenšteinas 302
Ekvivalentumo klasė pagal idealą 206
Elementai tarpusavyje pirminiai 213
Elementas algebrinis 259
– pirminis 211
– transcendentinis 224
– žiedo vienetinis 194
Elemento asocijuotas elementas 195
– atvirkštinis elementas 195
– daliklis 199
– kartotinis 199
Elementų santykis 222
Euklidas 56
Faktoržiedas 207
Ferma 7, 68
Forma simetrinė 307
Formulė Teiloro 284
Formulės Vieto 312
Funkcija Oilerio 66
– polinominė 229
Galia algebrinių skaičių aibės 381
– transcendentinių skaičių aibės 381
Galua 384
Gausas 68
Grandinė Šturmo 352
Homomorfizmas kanoninis 210
– žiedų 208
Homomorfizmo branduolys 209
– klasė 209
Horneris 249
Idealas, generuotas elementais 203
– komutatyviojo žiedo 202
– nulinis 202
– vienetinis 202
– vyriausiasis 203
Idealą generuojantys elementai 203
Idealų sankirta 204
– suma 204
Indeksas 177
Indeksavimas 179
Iracionalumas 271
Iracionalumo vardiklyje naikinimas 271
Integralumo sritis 199
Izomorfizmas 208
Kanoninis skaidinys polinomo 279
– – skaičiaus 43
Kartotinis elemento 199
– polinomo 347
– skaičiaus 6
Kartotinis bendrasis elementų 212
– – – mažiausias 213
– – polinomų 274
– – – mažiausias 274
– – skaičių 28
– – – mažiausias 28
Klasė liekanų 108

– pagal idealą 206
Kongruencija 101
Kriterijus Eizenšteino 302
– Oilerio 39
Lagranžas 94
Laukas algebriškai uždaras 260
– – neuždaras 260
– integralumo srities santykių 222
– polinomo skaidinio 279
– polinominių trupmenų 292
Lemos Gauso 299, 302
Liekana 12
– kvadratinė 156
Liekanų klasė 108
– pilnoji sistema mod *m* 112
– redukuotoji sistema mod *m* 114
Liuvilis 376
Lyginys mod *m* 101
– pagal idealą 205
Lygtis algebrinė 338
– – sangrąžinė 341
– Diofanto 36
– neapibrėžtoji 34
Metodas Hornerio 359
– intervalo dalijimo pusiau 355
– Lagranžo 357
Pirminis elementas 201
– polinomas 276
– skaičius 36
Plėtinys lauko 363
– – algebrinis 364, 372
– – – kartotinis 369
– – – paprastasis 365
– – transcendentinis 364
– – – paprastasis 365
– minimalusis 364
Polinomas kelių kintamųjų 238
– nulinis 255
– pirminis 276
– primityvusis 298
– sangrąžinis 341
– simetrinis 306
– – pagrindinis 307
– sudėtinis 276
– vieno kintamojo 225
Polinomo daliklis 247
– – kartotinis 289
– – tiesioginis 248
– – trivialusis 248
– išraiška leksikografinė 303
– išvestinė 283
– koeficientai 225
– laipsnis 225
–. narys 242
– normalusis pavidalas 242
– reikšmė 229, 246
– skaidinys kanoninis 279
– šaknis 253
– – kartotinė 255
Polinomo realiųjų šaknų atskyrimas 351
– – – skaičiaus nustatymas 351
Polinomai asocijuotieji 247
– tarpusavyje pirminiai 268
Polinomų atimtis 233
– daugyba 234
– lygybė algebrinė 225
– – funkcinė 230
– rezultantas 316
– sudėtis 232
– žiedas 236
– žiedų izomorfizmas 237
Polinominė funkcija 229, 246
– trupmena 292
– – nesuprastinamoji 292
– – paprasčiausioji 296
Reduktas grandininės trupmenos 77
Rodiklis skaičiaus mod *m* 167
Skaičiai tarpusavyje pirminiai 29
– tobulieji 52
Skaičiaus algebrinio laipsnis 260
– – minimalusis polinomas 365
– modulis 4
– sveikoji dalis 9
– trupmeninė dalis 9
Skaičius algebrinis 259
– transcendentinis 259
Skaičių faktorizacija 44
Šaknis polinomo 253
– – kartotinė 255
– – paprastoji 255
Šturmas 351
Šturmo grandinė 352
Teiloras 284
Teorema Abelio 384
– Bezu 252
– dalybos su liekana polinomų 261
– – – skaičių 11
– Euklido 56
– Ferma 122
– Liuvilio 377
– Oilerio 121
– pagrindinė simetrinių polinomų 307
– – klasikinės algebros 327
– polinomo šaknies egzistavimo 282
– Šturmo 353
Trupmena grandininė 75
– sisteminė baigtinė 185
– – begalinė 185
– – – periodinė 186
Žiedas 194
– Euklido 215
– komutatyvusis 194
– vyriausiųjų idealų 210
Žiedo charakteristika 196
– komutatyviojo idealas 202
Žiedų homomorfizmai 208

Turinys

Pratarmė 3

I skyrius. **Dalumo teorija sveikųjų skaičių žiede** 4

§ **1.** Sveikieji skaičiai ir jų veiksmai 4
§ **2.** Dalumo sąryšis sveikųjų skaičių žiede ir jo savybės 6
§ **3.** Dalikliai ir kartotiniai 8
§ **4.** Dalybos su liekana teorema. Euklido algoritmas 11
§ **5.** Skaičiavimo sistemos 15
§ **6.** Sistemos pagrindo keitimas 18
§ **7.** Didžiausias bendrasis daliklis ir mažiausias bendrasis kartotinis 23
§ **8.** Tarpusavyje pirminiai skaičiai 29
§ **9.** Neapibrėžtoji lygtis su dviem kintamaisiais 34
§ **10.** Pirminiai ir sudėtiniai skaičiai. Eratosteno rėtis 36
§ **11.** Pagrindinė aritmetikos teorema. Kanoninis skaidinys 41
§ **12.** Skaičiaus natūrinių daliklių skaičius ir suma 49
§ **13.** Pirminių skaičių pasiskirstymas 55
§ **14.** Čebyšovo nelygybė 57
§ **15.** Pirminių skaičių asimptotinis pasiskirstymas 62
§ **16.** Pirminiai skaičiai aritmetinėse progresijose 65
§ **17.** Kitos skaičių teorijos problemos 68

I skyrius. **Grandininės trupmenos** 74

§ **18.** Racionaliųjų skaičių skleidimas grandininėmis trupmenomis 74
§ **19.** Grandininių trupmenų reduktai 77
§ **20.** Reduktų savybės 81
§ **21.** Realiųjų skaičių skleidimas grandininėmis trupmenomis 84
§ **22.** Dirichlė teorema 87
§ **23.** Geriausieji artiniai 88
§ **24.** Periodinės grandininės trupmenos 91
§ **25.** Lagranžo teorema 94
§ **26.** Grandininių trupmenų taikymai 97

III skyrius. **Lyginiai** 101

§ **27.** Lyginio apibrėžimas. Pagrindinės lyginių savybės 101
§ **28.** Liekanų (likinių) klasės. Liekanų klasių žiedas 106
§ **29.** Liekanų sistemos moduliu m 112
§ **30.** Liekanų klasių, tarpusavyje pirminių su moduliu, grupė 116
§ **31.** Oilerio funkcijos reikšmių skaičiavimas 118
§ **32.** Oilerio ir Ferma teoremos 121
§ **33.** Lyginių taikymai 123

IV skyrius. **Lyginiai su kintamaisiais** 131

§ **34.** Lyginių su kintamaisiais sprendiniai 131
§ **35.** Pirmojo laipsnio lyginiai 134

§ **36.** Lyginių sistemos 141
§ **37.** Lyginiai moduliais, lygiais pirminio skaičiaus laipsniui 146
§ **38.** Lyginiai pirminiu moduliu 150
§ **39.** Kvadratiniai lyginiai 154
§ **40.** Oilerio ir Gauso kriterijai 157
§ **41.** Ležandro simbolis 161

V skyrius. **Laipsninės liekanos** 167

§ **42.** Rodiklis moduliu ir jo savybės 167
§ **43.** Primityviosios šaknys moduliu *m*. 171
§ **44.** Primityviųjų šaknų egzistavimas pirminiu moduliu. 174
§ **45.** Primityviosios šaknys sudėtiniu moduliu 176
§ **46.** Indeksai 177
§ **47.** Indeksų taikymai 181
§ **48.** Sisteminės trupmenos 185
§ **49.** Cikliniai periodo keitimai 191

VI skyrius. **Žiedai ir idealai** 194

§ **50.** Žiedas. Žiedo vienetas ir jo dalikliai 194
§ **51.** Integralumo sritis. Dalumo sąryšis integralumo srityje 198
§ **52.** Komutatyviųjų žiedų idealai 202
§ **53.** Lyginiai pagal idealą. Žiedo faktoržiedas 205
§ **54.** Žiedų homomorfizmai 207
§ **55.** Vyriausiųjų idealų žiedai 210
§ **56.** Vyriausiųjų idealų žiedo elementų didžiausias bendrasis daliklis ir mažiausias bendrasis kartotinis 212
§ **57.** Euklido žiedai 215
§ **58.** Integralumo srities santykių laukas 219

VII skyrius. **Polinomų virš integralumo srities žiedai** 224

§ **59.** Vieno kintamojo polinomai virš integralumo srities 224
§ **60.** Transcendentinio elemento egzistavimas. Polinomų aibės konstravimas . . 226
§ **61.** Algebrinė ir funkcinė polinomų lygybė 228
§ **62.** Operacijos vieno kintamojo polinomų aibėje 231
§ **63.** Kelių kintamųjų polinomų virš integralumo srities žiedai 238
§ **64.** Kelių kintamųjų polinomų normalusis pavidalas 240
§ **65.** Kelių kintamųjų polinomų žiedo konstravimas 245
§ **66.** Dalumo sąryšis polinomų virš integralumo srities žieduose 247
§ **67.** Hornerio schema 249
§ **68.** Vieno kintamojo polinomų šaknys 253
§ **69.** Polinomų virš nulinės charakteristikos integralumo srities algebrinės ir funkcinės lygybių ekvivalentumas 257
§ **70.** Algebriniai elementai 258

VIII skyrius. **Vieno kintamojo polinomų virš lauko žiedas** 261

§ **71.** Dalybos su liekana teorema 261
§ **72.** Polinomų bendrieji dalikliai. Polinomų didžiausias bendrasis daliklis . . . 265
§ **73.** Iracionalumo trupmenos vardiklyje naikinimas 271
§ **74.** Polinomų mažiausias bendrasis kartotinis 274
§ **75.** Pirminiai ir sudėtiniai polinomai. Sudėtinio polinomo išraiška pirminių polinomų sandauga 276
§ **76.** Polinomo šaknies egzistavimo teorema 280
§ **77.** Polinomų virš nulinės charakteristikos lauko išvestinės ir jų taikymai . . 283
§ **78.** Polinomo kartotinių daugiklių atskyrimas 289
§ **79.** Polinominių trupmenų laukas 292

IX skyrius. **Kelių kintamųjų polinomai** 298

§ **80.** Pirminiai ir sudėtiniai virš integralumo srities polinomai 298

§ **81.** Polinomo reiškimas formų suma. Polinomo leksikografinė išraiška 303
§ **82.** Simetriniai polinomai 306
§ **83.** Vieto formulės. Simetrinių polinomų pagrindinės teoremos išvados 312
§ **84.** Rezultantas ir jo taikymai 316

X skyrius. **Polinomai virš skaičių laukų** 327

§ **85.** Kompleksinių skaičių lauko algebrinis uždarumas 327
§ **86.** Polinomų su realiaisiais koeficientais kanoninis skaidinys 332
§ **87.** Polinomo su sveikaisiais koeficientais racionaliųjų šaknų savybės ir jų radimo algoritmas 333
§ **88.** Algebrinės lygtys 338
§ **89.** Polinomo su realiaisiais koeficientais realiųjų šaknų apytikslio radimo uždavinys 344
§ **90.** Intervalo, kuriame yra visos realiosios polinomo šaknys, ribų nustatymas . 346
§ **91.** Polinomo virš **R** realiųjų šaknų skaičiaus nustatymas ir šaknų atskyrimo Šturmo metodas 351
§ **92.** Polinomo su realiaisiais koeficientais realiųjų šaknų skaičiavimo artutiniai metodai 355

XI skyrius. **Laukų plėtiniai** 363

§ **93.** Transcendentiniai ir algebriniai lauko plėtiniai 363
§ **94.** Lauko paprastieji plėtiniai 365
§ **95.** Lauko kartotiniai algebriniai plėtiniai 369
§ **96.** Baigtiniai ir algebriniai plėtiniai 371
§ **97.** Algebrinių skaičių aibės savybės 373
§ **98.** Realiųjų transcendentinių skaičių egzistavimas 376
§ **99.** Algebrinių ir transcendentinių skaičių aibių galios 380
§ **100.** Apie algebrinių lygčių išsprendžiamumą radikalais. 382
§ **101.** Kubinių lygčių išsprendžiamumas kvadratiniais radikalais 384
§ **102.** Brėžimas skriestuvu ir liniuote 388
§ **103.** Pagrindinė brėžimo skriestuvu ir liniuote teorema 390
§ **104.** Keturių klasikinių brėžimo uždavinių neišsprendžiamumas 391
§ **105.** Aukštesniojo laipsnio Diofanto lygtys 394

Indeksų ir antiindeksų lentelės 400
Uždavinių atsakymai ir nurodymai 405
Literatūra 409
Dalykinė rodyklė 410

Bulota K., Survila P.

Bu236 Algebra ir skaičių teorija: Vadovėlis ped. inst. matematikos spec.— 2-asis patais. ir papild. leid.— V.: Mokslas, 1989—1990.

[D.] 2.— 416 p. ISBN 5-420-00613-8

Vadovėlio antroje dalyje dėstoma sveikųjų skaičių dalumo teorija, polinomų žiedai, lyginių teorija, gvildenama polinomų šaknų egzistavimas ir radimas, lygčių išsprendžiamumas, skaičių laukų plėtiniai. Pateikiama pavyzdžių ir uždavinių.

B $\frac{1602040000-142}{M854(08)-90}$ 79—90

UDK 512(075.8)+511.2(075.8)

Учебное издание. **Булота** Антанас-Кястутис, **Сурвила** Пранас. АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ. Ч. 2. Допущено Министерством образования и культуры Литвы в качестве учебника для студентов пед. ин-тов. Издание 2-е, переработанное и дополненное. Вильнюс, «Мокслас», 1990. На литовском языке

Mokymo leidinys. **Bulota** Antanas Kęstutis, **Survila** Pranas. ALGEBRA IR SKAIČIŲ TEORIJA. D. 2. Redaktorė E. Leikauskienė. Viršelio dailininkas ir meninis redaktorius V. Ajauskas. Techninė redaktorė A. Gineitienė. Korektoriai: L. Balaikienė ir V. Stepšys

ИБ № 3383

Duota rinkti 1990 02 20. F. Pasirašyta spaudai 1990 08 03. SL. 256. Formatas 60×90¹/₁₆. Popierius — spaudos Nr. 2. Garnitūra —„Romaniška", 10 punktų. Iškilioji spauda. 26 sąl. sp. l. 26,25 sąl. spalv. atsp. 28,77 apsk. leid. l. Tiražas 4000 egz. Užsakymas 518. Kaina 1 rb 20 kp.
„Mokslo" leidykla. 232050 Vilnius, Žvaigždžių 23.
Spaudė Spindulio spaustuvė. 232000 Kaunas, Gedimino 10